ICT GEDRAGSCODE

december 2019

Informatie- en communicatietechnologie en middelen zoals computer, e-mail, internet, gsm, … zijn cruciaal geworden in onze huidige werking. We streven naar een efficiënte, doelgerichte en klantvriendelijke dienstverlening en ICT speelt hierin een voorname rol. Het bestuur investeert dan ook graag in de uitbouw

van ICT middelen. Het is aan ieder van ons om deze middelen op een goede, efficiënte en verantwoorde wijze te gebruiken.
Deze gedragscode biedt u hiertoe de nodige richtlijnen.

Inhoud

Toepassingsgebied ICT code

Voor wie?

Deze ICT gedragscode geldt voor iedereen die binnen het lokaal bestuur activiteiten verricht. De code is dan ook van toepassing op

- alle personeelsleden van gemeente en OCMW Beveren, incl. onderwijzend personeel
- alle medewerkers in tijdelijk dienstverband (vb. stagiairs, jobstudenten, …)
- derden die toegang hebben tot de elektronische communicatiemiddelen van het lokaal bestuur (bijvoorbeeld externe ICT-technici voor onderhoud aan serverpark, …).

Voor de medewerkers van de ICT dienst geldt een bijkomende gedragscode.

Werk – privé gebruik

Deze gedragscode regelt het gebruik van de elektronische communicatiemiddelen die het bestuur u ter beschikking stelt, ook indien u deze middelen inzet voor privé gebruik (zoals bijvoorbeeld het gebruik van een gsm voor privé-gesprekken, …)

Deze gedragscode is goedgekeurd door het bestuur en is van toepassing vanaf 1 januari 2020. De code zit vervat als bijlage bij het arbeidsreglement. De algemeen directeur of zijn plaatsvervanger waakt over de naleving van deze gedragslijn.

Wat is ICT?

ICT staat voor informatie- en communicatietechnologie.
Deze gedragscode is van toepassing op alle ICT-middelen en gegevens die de aanstellende overheid ter beschikking stelt van de personeelsleden.

Onder "ICT middelen" verstaan we alle middelen die een rol vervullen in informatie- en communicatieprocessen. Het gaat hierbij onder meer om:

- Apparatuur:
  - computers (zowel vast als draagbaar)
  - telefoons (zowel vast als mobiel, smartphones,….
  - kopieertoestellen / multifunctionals / printers
  - beamers
  - USB-sticks, internetsticks
  - …
- Netwerken: interne en externe (eventueel draadloze) netwerken inclusief internet
- Programma's en toepassingen die het mogelijk maken gegevens te raadplegen, verwerken, opslaan en verzenden
  - Web
  - e-mail
  - (interne en externe) databanken
  - Apps
  - …

Elektronische documenten: alle informatie in digitale vorm zoals bijvoorbeeld e-mail, websites, tekstbestanden, foto's, muziek, video's, geluidsfragmenten,…

De elektronische communicatiemiddelen zijn en blijven te allen tijde eigendom van het lokaal bestuur. Deze kan dan ook beslissen om alle of bepaalde communicatiemiddelen tijdelijk of permanent niet langer ter beschikking te stellen van het personeelslid (de gebruiker), dan wel om beperkingen op te leggen aan het gebruik daarvan.

Onder "gegevens" verstaan we:

Alle informatie die zich, al dan niet tijdelijk, op ICT-middelen van het lokaal bestuur bevindt. Dit is alle informatie die u maakt, ontvangt, vermenigvuldigt, wijzigt en/of verstuurt door gebruik te maken van elektronische communicatiemiddelen (al dan niet eigen, van de werkgever, of van derden). Ook afdrukken op papier van deze gegevens dienen adequaat beschermd te worden.

Uitgangspunt: geoorloofd en ongeoorloofd gebruik

Deze gedragscode is gebaseerd op het geoorloofd en ongeoorloofd gebruik van ICT.

De ICT-middelen en gegevens die het lokaal bestuur u ter beschikking stelt, mogen alleen gebruikt worden voor doeleinden die bijdragen tot het verrichten van de overeengekomen arbeid. Tijdens de werkuren moet u zich als personeelslid volledig aan uw job wijden en mag u geen ongeoorloofd gebruik maken van uitrusting of materiaal van het bestuur.

Ongeoorloofd gebruik is ruimer dan illegaal gebruik. Onder ongeoorloofd gebruik verstaan we elke vorm van gebruik waarvan de medewerker weet of hoort te weten dat het voor de organisatie ontoelaatbaar is. Voorbeelden daarvan zijn:

- Veelvuldig privé-telefoongebruik
- Het gebruiken van kopieerapparatuur voor privédoeleinden
- Het verzenden en ontvangen van privé-informatie per e-mail
- Het via internet bekijken of downloaden van informatie voor privégebruik
- Bekijken, downloaden, verzenden of ontvangen van pornografisch, erotisch, racistisch, extremistisch en/of discriminerend materiaal
- Bekijken of beluisteren van streaming audio en video van bijvoorbeeld life music en bewegende beelden (tenzij in het kader van een e-cursus of opdracht, denk aan de programmator cultuurcentrum bij de samenstelling van het jaarprogramma, …)
- Gebruik van sociale netwerksites voor privédoeleinden (Facebook, Instagram, LinkedIn, Twitter, …)
- Downloaden of spelen van spelprogramma's
- Veelvuldig gebruik van PC en printer voor privédoeleinden
- Verstrekken van privacy of bedrijfsgevoelige informatie vanuit informatiesystemen/ databanken aan onbevoegden

De leidinggevende ziet toe op het ongeoorloofde gebruik. Indien de leidinggevende ongeoorloofd gebruik constateert, onderneemt hij/zij actie overeenkomstig de aard van het geconstateerde feit.
(zie verder rubriek "Toezicht en controle")

Een beperkt en occasioneel privégebruik van de ICT-middelen die u ter beschikking zijn gesteld is toegestaan op voorwaarde dat dit gebruik:

- niet geschiedt tijdens je werktijden, tenzij in geval van dringende noodzaak;
- niet storend is voor de goede werking van het bestuur, de dienstverlening, de collega's en eigen taken van het personeelslid;
- niet leidt tot kosten voor het bestuur die in alle redelijkheid te hoog zijn.

In de mate waarin privégebruik is toegestaan, is dit een gunst en geen recht.

Algemene richtlijnen

Goede huisvader

U bent verantwoordelijk voor de ICT-apparatuur die u ter beschikking gesteld wordt. Deze apparatuur
- moet u in goede staat houden
- mag u niet onbeheerd achterlaten.

U respecteert de door het lokaal bestuur getroffen veiligheidsmaatregelen (vb. toegangscontrole) om zo diefstal en beschadiging te voorkomen. Mocht u toch het slachtoffer zijn van een diefstal moet u dit onmiddellijk melden aan de ICT dienst, dienst verzekeringen en uw leidinggevende.

Wetgeving

U zorgt ervoor dat informatieverwerking en communicatie steeds in overeenstemming met de wet worden verricht.

Zo is bijvoorbeeld zeker niet toegelaten:

- informatie te verspreiden, verwerken of op te slaan in strijd met de geldende wetgeving, zoals de bepalingen van de Algemene Verordening Gegevensbescherming (AVG/GDPR);
- programmatuur te installeren of te gebruiken waarvoor de bevoegde autoriteit geen toestemming heeft verleend of waarvan het gebruik in strijd is met de licentievoorwaarden;
- informatie te verwerken of te verspreiden in strijd met de wetgeving over het auteursrecht en andere intellectuele rechten (bijvoorbeeld: illegale muziek of films afspelen of downloaden);
- informatie te verwerken of te verspreiden die in strijd is met de wetgeving ter bestrijding van het racisme of die in het algemeen beledigend of lasterlijk is voor andere personen;
- informatie te verwerken of te verspreiden die strijdig is met de wetgeving over de bescherming van de goede zeden;
- informatie te verwerken of te verspreiden die schade kan toebrengen aan derden.

Telewerken /tijds- en plaats onafhankelijk werken

Door de toename van tijds- en plaats onafhankelijk werken en de moderne communicatiemogelijkheden zijn de grenzen tussen privé en werk vaak minder duidelijk. Medewerkers kunnen, indien men voldoet aan een aantal voorwaarden, occasioneel of structureel telewerken. De werkgever stelt een laptop ter beschikking, eventuele andere benodigde apparatuur (bv. printer) moet u zelf voorzien. De laptop blijft eigendom van gemeente Beveren. Als u documenten en materiaal mee op verplaatsing neemt (bv. naar huis), treft u de nodige maatregelen om die informatie te beschermen, zowel thuis als onderweg. Respecteer de bestaande afspraken binnen de organisatie en binnen uw dienst. Meer inlichtingen over telewerken, vindt u terug in het reglement telewerk.

Imago & deontologie

U gebruikt elektronische communicatiemiddelen om in naam van het lokaal bestuur te communiceren. Uw werkgever verwacht dan ook dat u bij het communiceren klantvriendelijk, beleefd, …bent en steeds aandacht heeft voor gepast taalgebruik en correcte spelling.

U dient bij het verwerken en verspreiden van informatie rekening te houden met de belangen en gevoeligheden van het bestuur en haar medewerkers.

Let op voor:

- informatie die het imago van het lokaal bestuur schendt of haar in het algemeen zowel moreel als economisch kan schaden;

- informatie die een pornografisch of uitgesproken erotisch karakter heeft, discriminerend of aanstootgevend is of kan zijn voor anderen omdat ze tegen de algemeen geldende fatsoenregels indruist;
- informatie die als vertrouwelijk betiteld wordt of die wegens de aard ervan redelijkerwijs als vertrouwelijk moet beschouwd worden, zoals persoonlijke gegevens, tenzij men die informatie in het kader van de toegewezen opdracht moet behandelen.

Label

Heel wat ICT-objecten zijn opgenomen in een inventaris. Ze kregen allemaal een uniek identificatienummer, terug te vinden op één of meerdere labels op het toestel. Via het nummer en de inventaris kan de ICT dienst de geschiedenis van het object (eventueel wederkerende mankementen, levensduur, …) opvolgen.

- U mag deze labels niet verwijderen of verplaatsen.
- U mag geen eigen labels of herkenningstekens aanbrengen.
- Indien een label is verdwenen, moet u dit melden aan de dienst informatica

U mag toestellen (vb. computers) ook niet naar een andere werkplek verplaatsen tenzij mits uitdrukkelijke toestemming van de ICT dienst.

Toezicht en controle

Binnen de wettelijke grenzen kan het lokaal bestuur controle uitoefenen op gegevens die een personeelslid opslaat, verstuurt of ontvangt binnen het toepassingsgebied van deze richtlijnen. Zij respecteert het recht van het personeelslid op bescherming van de persoonlijke levenssfeer in het kader van de dienstbetrekking. Zij verbindt zich ertoe haar controle uit te voeren in het licht van de bepalingen van de Algemene Verordening Gegevensbescherming (AVG/GDPR).

De controle zal gebeuren op een wijze die de inmenging in de persoonlijke levenssfeer tot een minimum beperkt.

Systeembeheerders spelen hierbij een grote rol. Zij zijn verantwoordelijk voor de goede werking van de computersystemen. Hun taken zijn onder andere het maken van back-ups, het installeren en instellen van updates van een besturingssysteem, het installeren en instellen van hardware en software, het toevoegen/wijzigen/ verwijderen van gebruikersinformatie, het opnieuw instellen van wachtwoorden, het beantwoorden van technische vragen, de beveiliging van het netwerk, het documenteren van de werking van het systeem, het onderzoeken en oplossen van gemelde problemen, garanderen dat services permanent actief zijn ...

Procedure

1. De systeembeheerders 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 veiligheidsproblemen te voorkomen. Deze controles kunnen slechts uitgevoerd worden door geautoriseerde systeem-beheerders. Alle medewerkers moeten zich bewust zijn van het bestaan van deze controlemogelijkheid en van het feit dat alle communicatie die zij via het netwerk uitwisselen, hieraan onderworpen kan worden.
2. De organisatie mag het gebruik van de elektronische communicatiemiddelen op een globale wijze controleren. Zo mag een globaal overzicht, eventueel per organisatorische entiteit, van de gedurende een bepaalde periode bezochte websites alsook de frequentie en het volume van de doorgezonden informatie, zonder daarin op enige wijze gegevens over het individueel gebruik op te nemen. Gezien de specifieke wetgeving worden de logins op het bevolkingsbestand gecontroleerd door de coördinator Bevolking of het diensthoofd Burgerzaken.
3. Indien de systeembeheerders naar aanleiding van controletaken vaststellen dat een of meer gebruikers bewust of onbewust de veiligheid of de goede werking van het systeem in het gedrang brengen, brengen ze de algemeen directeur en de functionaris gegevensbescherming (DPO) onmiddellijk op de

hoogte. Na overleg mogen zij deze gebruikers identificeren en, indien nodig, contacteren om de problemen te verhelpen. Zij mogen de activiteiten van deze gebruikers, indien noodzakelijk en na verwittiging, ook verder opvolgen om herhaling van het probleem te voorkomen.

4. Het gebruik van communicatiemiddelen in het bestuur wordt, buiten het zopas vermelde geval, niet systematisch op individuele wijze gecontroleerd.
5. Vaststelling ongeoorloofd gebruik
   5.1. Indien de systeembeheerders ongeoorloofd gebruik vaststellen dat een misdrijf uitmaakt of op ernstige wijze de financiële of economische belangen van de organisatie in het gedrang brengt, kunnen de betrokken gebruikers verder, zonder verwittiging, gecontroleerd worden met het oog op het verzamelen van bewijsstukken.
   5.2. In andere gevallen van ongeoorloofd gebruik wordt een waarschuwings-procedure in acht genomen die hoofdzakelijk tot doel heeft de medewerker(s) op de hoogte te brengen van een onregelmatigheid en van het feit dat in de toekomst systematische en individuele controle zal plaatshebben wanneer een nieuwe onregelmatigheid wordt vastgesteld.

   5.3. De volgende procedureregels worden hierbij in acht genomen:
      - De systeembeheerders brengen na het vaststellen van vermoedelijk ongeoorloofd gebruik onmiddellijk de algemeen directeur op de hoogte.
      - De algemeen directeur beoordeelt de vaststelling en maakt uit of procedure 5.1 of 5.2 van tel is.
      - In het laatste geval wordt de voor de onregelmatigheid verantwoordelijk geachte medewerker uitgenodigd voor een gesprek.
      - Dit gesprek heeft plaats voor iedere beslissing of evaluatie die de medewerker individueel kan raken.
      - Het gesprek heeft tot doel de medewerker de kans te bieden zijn bezwaren met betrekking tot de voorgenomen beslissing of evaluatie uiteen te zetten en hem verantwoording te vragen over zijn gebruik van de hem/haar ter beschikking gestelde communicatiemiddelen.

Behandeling van incidenten

Meldingsplicht

1. Alle gebruikers hebben de verantwoordelijkheid om inbreuken op deze gedragscode te melden. U meldt deze aan uw respectievelijk diensthoofd, afdelingshoofd of de algemeen directeur / zijn plaatsvervanger.
2. Indien een hiërarchische overste een inbreuk vaststelt, kan hij/zij dit rechtstreeks aan de algemeen directeur of zijn plaatsvervanger melden.
   De algemeen directeur of zijn plaatsvervanger kan een tuchtprocedure inleiden.
3. Indien de systeembeheerders een incident vaststellen, informeren zij onmiddellijk de algemeen directeur of zijn plaatsvervanger.

Maatregelen

1. In afwachting van een definitieve maatregel kan de algemeen directeur of zijn plaatsvervanger voorlopige maatregelen treffen om ernstigere problemen te voorkomen.
2. Bij twijfel over de ernst van de inbreuk of over de aard van de sanctie kan de hiërarchische overste, in alle discretie, het advies van de systeembeheerders inwinnen.
3. Bij vaststelling van overtredingen op de gedragscode kan bij wijze van (een) voorlopige bewarende maatregel(en), minstens één van de volgende stappen ondernomen worden om de veiligheid en integriteit van de systemen en de gegevens te waarborgen:
   - De hiërarchische oversten van de gebruiker worden van de situatie op de hoogte gesteld, als dit nog niet gebeurd is.

- De toegangsrechten van de gebruiker kunnen gedurende het onderzoek opgeschort of beperkt worden (bijvoorbeeld ontzeggen of beperken van de toegang tot het netwerk of de computersystemen, …)

bestanden, cd's, usb-sticks en andere informatiedragers van de betrokken gebruiker kunnen worden geïnspecteerd.

Sancties en beroepsmogelijkheid

Mogelijke sancties zijn:

- al dan niet tijdelijke beperking in de toegang tot bepaalde communicatiemiddelen;
- tijdelijk of definitief verbod tot het gebruik van bepaalde communicatiemiddelen;
- betalen van de kosten voortvloeiend uit het misbruik;
- indien het misbruik een strafrechtelijk misdrijf uitmaakt kan de betrokkene voor die feiten gerechtelijk vervolgd worden, ongeacht eventuele schade-vorderingen. Het lokaal bestuur zal meewerken bij het opsporen van dergelijke misdrijven, en zal eventuele gebruikersgegevens en bestanden overmaken aan de gerechtelijke instanties wanneer hierom verzocht wordt;
- het inleiden van een tuchtprocedure.

Elk personeelslid heeft de mogelijkheid beroep aan te tekenen tegen de beslissing en maatregelen die getroffen worden bij vaststelling van een inbreuk op deze gedragscode. Dit beroep dient schriftelijk binnen de 30 dagen overgemaakt te worden aan het college van burgemeester en schepenen/vast bureau.

Tot slot

Contactpersoon

Voor vragen over de toepassing van deze gedragscode en verduidelijking van technische termen kan u terecht bij uw diensthoofd en onderstaande diensten:

- Medewerkers ICT dienst: tel. 03 750 16 80
- Medewerkers personeelsdienst: tel. 03 750 16 50
- Functionaris Gegevensbescherming: tel. 03 750 46 14

Meldingen in verband met het ongeoorloofd gebruik van de elektronische communicatiemiddelen binnen het bestuur en overtreding van deze gedragscode moeten worden gemeld aan uw diensthoofd, afdelingshoofd, de algemeen directeur of zijn plaatsvervanger.

Werknemers die via elektronische communicatiemiddelen het slachtoffer zijn van pesterijen, ongewenst seksueel gedrag of ander storend gedrag (vb. overdreven aantal mails, "stalking", …) kunnen zich ook tot de vertrouwenspersonen wenden. Een overzicht van de vertrouwenspersonen kan u terugvinden op het intranet.

Het bestuur garandeert een strikt vertrouwelijke behandeling van alle klachten

Evaluatie en bijsturing

De richtlijnen in dit document hebben betrekking op communicatiemiddelen die voortdurend evolueren. Deze gedragscode zal daarom in de toekomst aangevuld of aangepast worden. Alle belangrijke wijzigingen worden meegedeeld.
Vragen, opmerkingen en suggesties zijn welkom op de ICT dienst of op de personeelsdienst.

Akkoord

Elk personeelslid tekent voor ontvangst van dit document op de laatste pagina van deze bundel.

BIJLAGE:
Het ABC van de ICT-gedragscode

AFWEZIGHEIDSASSISTENT

- Indien u langer dan één dag afwezig bent, schakel dan uw afwezigheidsassistent in. De afwezigheidsassistent bevat volgende informatie:

Binnen de organisatie:

Geachte mevrouw / heer

Ik ben afwezig tot dag maand. Uw mail lees ik pas op dag maand. Voor dringende zaken kunt u steeds terecht bij de collega's van dienst x op tel.
03 750 xx xx of dienst@beveren.be

autohandtekening

Buiten de organisatie:

Geachte mevrouw / heer

Ik ben afwezig tot dag maand. Uw mail lees ik pas op dag maand. Voor dringende zaken kunt u steeds terecht bij naam collega. U kan haar/hem bereiken op het nummer x of via xx@beveren.be.

autohandtekening

- Voor een niet-geplande afwezigheid (vb. door ziekte) die langer dan 3 dagen duurt, dient in samenspraak met het personeelslid binnen de dienst een regeling getroffen te worden zodat ingekomen e-mails tijdig kunnen worden behandeld. (of indien niet mogelijk met de ICT dienst).
  Via https://owa.beveren.be/ kan u uw mailbox via internet raadplegen. Zo kan u bij ziekte ook van thuis uit uw afwezigheidsassistent aanzetten (zie opties).

BEAMER

Heel wat vergaderzalen in het gemeentehuis zijn standaard uitgerust met een beamer en scherm. Indien nodig kan u op de ICT dienst het nodige materiaal ontlenen zoals een beamer, verlengkabel, eventueel netwerkkabel, laserpen voor aanduiding op een scherm,…
U doet dit via een melding in Topdesk (zie p.20)
Let op: de collega's van de ICT dienst stellen het materiaal zelf niet op!

Geeft u een presentatie in het cultuurcentrum Ter Vesten dan zorgen de collega's van cc Ter Vesten (tel. 03 750 10 00) voor een beamer, scherm, …

Let op: de reservatie van een scherm (voor gebruik op externe locaties) loopt niet via de ICT dienst. Hiervoor kan u terecht bij de communicatiedienst, tel. 03 750 15 80

BEVEILIGING

Enkel via individuele authenticatie (login, wachtwoord, eventueel toegang via elektronische identiteitskaart) krijgt u toegang tot de computerinfrastructuur en de communicatiemiddelen van de organisatie.

Elk personeelslid is verantwoordelijk en aansprakelijk voor alles wat onder zijn/haar gebruikersidentificatie gebeurt. Het wachtwoord is individueel en geheim. Zo ook andere inlogmiddelen zoals het eID met de PIN code als paswoord, tokens, bankpassen.

- Uw login wordt aangemaakt door de ICT dienst.
- Uw wachtwoord is strikt **persoonlijk en geheim**.
  U mag niet werken met een login en/of paswoord van anderen. Geef uw wachtwoord nooit door (zeker niet via mail of toepassingen die daar op een min of meer officiële wijze zouden om vragen). Let vooral op foutmeldingen bij het ingeven van wachtwoorden en wanneer u opnieuw wordt gevraagd om uw wachtwoord in te geven.
- Uw wachtwoord moet aan volgende **voorwaarden** voldoen:

  Wachtwoorden dienen minimaal 10 karakters te bevatten.
  Wachtwoorden dienen minimaal 1 cijfer te bevatten.
  Wachtwoorden dienen minimaal 1 non-alfanumerieke waarde te bevatten (bv: !@#$%^&)*
  Wachtwoorden mogen niet gelijk zijn aan usernamen of domeinnamen.
  Wachtwoorden mogen niet voor de hand liggend te zijn.
  Wachtwoorden dienen om de 2 maanden gewijzigd te worden:
  Wachtwoorden mogen niet hergebruikt worden binnen het jaar.

- U heeft de mogelijkheid om op eender welk tijdstip zelf uw wachtwoord te **wijzigen** doch dit moet minstens om de 2 maanden gebeuren.
- Een vervallen wachtwoord wordt best nooit opnieuw gebruikt. Het systeem verhindert trouwens een van de laatste 5 gekozen wachtwoorden opnieuw te gebruiken.
- Als u uw **wachtwoord vergeten** bent, moet u contact opnemen met de ICT dienst om een nieuw wachtwoord te ontvangen. Dit nieuwe wachtwoord moet u meteen na ontvangst wijzigen. De informaticaverantwoordelijken mogen immers nooit het wachtwoord van een gebruiker kennen.
- Het is **verboden**:
  - een wachtwoord in te typen wanneer een andere persoon meekijkt.
  - te kijken wanneer iemand zijn wachtwoord intypt.
  - andermans wachtwoorden proberen te weten te komen op welke manier dan ook.

  Het kraken van wachtwoorden of inbreken in computers is een misdrijf.
- Bij het minste vermoeden dat het wachtwoord **ontvreemd** werd of ter kennis is van een medewerker of derde, moet u onmiddellijk uw wachtwoord vervangen én uw leidinggevende en de ICT dienst (systeembeheerders) over het eventuele misbruik inlichten.
- Wanneer de computer de vraag stelt om het wachtwoord te bewaren op het scherm, moet u steeds **negatief** antwoorden.
- Het wachtwoord dat u gebruikt om toegang te krijgen tot het netwerk mag niet gebruikt worden om toegang te krijgen tot **internetsites** die een registratie van login en wachtwoord vereisen. Het is immers zo dat malafide personen of organisaties via allerlei technieken aan deze cruciale informatie geraken en zo cyberaanvallen kunnen inzetten op ons netwerk.
- Daar wachtwoorden op documenten niet gewist kunnen worden, is het beveiligen van originele (office) **documenten** met een wachtwoord niet toegestaan (tenzij als maatregel om het document te beveiligen bij verzending).
- Wij raden u aan uw computer **nooit zonder toezicht** te laten, aangezien om het even wie dan kan handelen in naam van de aangemelde gebruiker. Wanneer u het lokaal verlaat, moet u steeds ofwel de computer vergrendelen, ofwel zich afmelden door uit te loggen op de computer. Dit kan op een snelle manier door de **sneltoets "windowstoets"** in te drukken **samen met de letter L**.

- De **schermbeveiliging** moet met het wachtwoord beveiligd zijn en moet ook steeds ingesteld staan zodat deze automatisch in werking treedt binnen de 20 minuten. Deze schermbeveiliging volstaat echter niet om aan de bovenstaande richtlijn te voldoen. Ze fungeert enkel als noodoplossing voor het geval een gebruiker zelf manueel zijn computer is vergeten te vergrendelen.
- U dient toegangsmiddelen zoals pasjes voor bankieren, VPN tokens, … altijd **gescheiden te bewaren** van het bijhorende ICT-middel (eID-lezer, laptop, …) om bij verlies of diefstal de risico's te beperken. Het spreekt vanzelf dat de bijbehorende pin-code of het wachtwoord zeker niet bij het ICT middel of het toegangsmiddel mag bewaard worden. Schrijf wachtwoorden ook niet op!
- U mag de **antivirus**software op uw PC of laptop niet uitschakelen. Gezien het groot belang van het correct gebruik van antivirussoftware voor de gemeentelijke organisatie wordt het gebruik hiervan ook te allen tijde gelogd.
- Als u geconfronteerd wordt met een **virus** contacteert u onmiddellijk de ICT dienst. Wie een **verdacht** elektronisch bericht of bestand toegezonden krijgt, kan de ICT dienst hiervan best op de hoogte brengen.
- Indien het netwerk geconfronteerd wordt met een **virus**, zal de ICT dienst u misschien vragen om zelf dringende opdrachten op uw PC uit te voeren. U dient deze opdrachten steeds onmiddellijk uit te voeren! Indien u de instructies niet begrijpt, kan u steeds de ICT dienst contacteren voor bijkomende inlichtingen.

CAMERA

Onder cameratoezicht verstaan we elk bewakingssysteem met één of meerdere camera's dat ertoe dient om vanop afstand bepaalde plaatsen af activiteiten van de werkplek te bewaken met of zonder het oog op bewaring van de beeldgegevens die het inzamelt en overbrengt.

Cameratoezicht zal enkel worden uitgeoefend voor het nastreven van één van de volgende doeleinden:

- De veiligheid en gezondheid
- De bescherming van de goederen van het bestuur (en haar klanten)
- De controle van het arbeidsproces, de arbeid van de personeelsleden, met het oog op de evaluatie en verbetering van de werkorganisatie.

Het bestuur zal de personeelsleden of hun vertegenwoordiging er schriftelijk over inlichten wanneer zij effectief overgaat tot camerabewaking en zal de wettelijke verplichtingen terzake naleven. Het bestuur zal hen dan minstens informatie verschaffen over

- Het nagestreefde doel van het cameratoezicht
- Het feit of de beeldgegevens al dan niet bewaard worden
- Het aantal en de plaatsing van de camera('s)
- De betrokken periode gedurende dewelke de camera('s) functioneert/functioneren.

Het bestuur zal bij het cameratoezicht niet verder gaan dan redelijkerwijs nodig is om aan de meegedeelde doeleinden te voldoen. Het toezicht zal steeds, uitgaande van de doeleinden, toereikend, ter zake dienend en niet overmatig zijn. Indien de verkregen beelden gebruikt worden voor andere doeleinden dan deze waarvoor het cameratoezicht ingevoerd werd, dan moet het bestuur ervoor zorgen dat dit gebruik verenigbaar is met de oorspronkelijke doeleinden.

Het cameratoezicht zal er in elk geval nooit specifiek op gericht zijn om een bepaald personeelslid permanent in beeld te houden.

DATALEKKEN

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG of GDPR) van kracht. Deze Europese Verordening brengt nieuwe verplichtingen met zich mee in geval van een inbreuk in verband met persoonsgegevens, ook wel datalek genoemd.

“Een datalek bestaat wanneer er een inbreuk is op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden of opgeslagen gegevens met betrekking tot een geïdentificeerde of identificeerbare natuurlijke persoon (art. 4, 12 AVG).”

Het betreft dus zeker niet alleen de gevallen waarbij personen te kwader trouw (hackers) persoonsgegevens proberen te bemachtigen of de toegang ertoe blokkeren door de persoonsgegevens te encrypteren door middel van ransomware.

Hoewel aan die laatste categorie van aanvallen steeds veel media-aandacht wordt besteed, gebeuren meer dan 80% van de datalekken als het ware ‘per ongeluk’.

Typische voorbeelden zijn:

- het verliezen van een smartphone of USB-stick waarop een document staat met de namen van alle personeelsleden, cliënten of gegevens van burgers;
- het versturen van een document met persoonsgegevens per e-mail naar een externe persoon of zelfs naar een persoon binnen de onderneming waarvan wordt verondersteld dat deze daar geen toegang toe moet hebben in het kader van zijn functie;
- het crashen van een computer met als gevolg dat alle gegevens verloren zijn en er geen back-up bestaat van persoonsgegevens wordt beschouwd als een datalek.

Los van de operationele gevolgen waar een organisatie mee te kampen krijgt als gevolg van een datalek, brengt een dergelijke inbreuk verplichtingen met zich mee in het kader van de AVG. De verwerkingsverantwoordelijke moet binnen de 72 uur nadat deze kennis heeft genomen van het lek, de Gegevensbeschermingsautoriteit informeren.

Daarom is het belangrijk dat ieder personeelslid dat een datalek vaststelt dit zo snel mogelijk doorgeeft aan de DPO. Het melden van een datalek kan op twee manieren:

- *Interne melding:* **via Topdesk.**
  Bij een interne melding wordt gevraagd zoveel mogelijk informatie over het datalek (wat, wie, wanneer, waar) mee te geven. Deze melding komt rechtstreeks terecht bij de functionaris gegevensbescherming (DPO) van de organisatie.
- *Externe melding:* via privacy@beveren.be.
  Via deze weg kunnen burgers, leveranciers en medewerkers die geen toegang hebben tot Topdesk een datalek doorgeven.

DISCLAIMER

Aan elk uitgaand bericht zal automatisch een link naar www.beveren.be , facebook en Twitter en disclaimer toegevoerd worden.

Het bestuur kan deze verplichte vermeldingen wijzigen. De laatste versie is steeds terug te vinden op de website: https://www.beveren.be/disclaimer-mailverkeer

GSM

Zie telefonie

INTERNET

Het gebruik van internet tijdens de kantooruren voor niet-professionele doeleinden, zorgt voor een vermindering van de reëel geleverde prestaties en een vermindering van de kwaliteit van de dienstverlening.

Een beperkt en occasioneel privégebruik is toegestaan op voorwaarde dat dit gebruik:

- niet gebeurt tijdens de werktijd van de medewerker;
- niet storend is voor de goede werking van het bestuur, de dienstverlening, de collega's en de eigen taken;
- geen storende gevolgen heeft voor de werking van het netwerk;
- niet leidt tot kosten voor het bestuur die in alle redelijkheid te hoog zijn.

In de mate dat privégebruik is toegestaan, is dit een gunst en geen recht. Het bestuur kan te allen tijde het privégebruik verder inperken of afschaffen, in het bijzonder wanneer u als personeelslid deze gedragscode of bijkomende instructies van het bestuur niet naleeft.

Het bestuur heeft het recht om de toegang van bepaalde websites af te sluiten.

Onbeperkte toegang

Het bestuur heeft ervoor gekozen om alle personeelsleden haast onbeperkt toegang te geven tot het internet. Via een samenwerking met Proximus wordt een filter toegepast die enkele soorten sites afschermt zoals pornosites (zie verder).
Heel wat collega's hebben internet nodig voor de kwaliteitsvolle uitoefening van hun functie. We rekenen er dan ook op dat iedereen efficiënt met dit middel omspringt.

Ongeoorloofd gebruik internet

Volgende handelingen op het internet zijn ongeoorloofd:

- cyberpesten;
- deelnemen aan chatrooms en nieuwsgroepen die geen aantoonbaar belang hebben met uw functie;
- bekijken, downloaden, verzenden of ontvangen van pornografisch, erotisch, racistisch, extremistisch of discriminerend materiaal;
- bekijken of beluisteren van streaming audio en video (life music, bewegende beelden – tenzij voor een e-cursus of voor de uitoefening van een opdracht zoals het bekijken van mogelijke artiesten voor cultuurprgrammatie;
- downloaden of spelen van spelprogramma's.

KOPIEREN EN PRINTEN

Er staan op elke verdieping multifunctionele printers. Je kan op alle printers afdrukken.

De multifunctionals zijn zo ingesteld dat de follow-me functionaliteit de standaard is. Dit betekent dat je je printopdracht op elke multifunctional en vanop elke locatie kan afdrukken met je badge. Om deze follow-me functionaliteit te gebruiken, moet je identificatiebadge eenmalig gekoppeld worden aan je gebruikersnaam.

In geval van storingen meld je dit aan een van de key-users van de multifunctionals.

Het aanvullen van de papierlades en vervangen van de toners gebeurt door iedereen die merkt dat ze leeg zijn. Dit is een kwestie van respect voor je collega's. Het onderhoud van de printers gebeurt door de leverancier.

De multifunctionals worden niet gebruikt voor privédoeleinden.

b) Afdrukken

Druk zo weinig mogelijk documenten af.

Als je toch moet afdrukken, hanteer dan volgende principes:

- documenten druk je zoveel mogelijk recto-verso af;

- meestal is een document nog perfect leesbaar als je 2 pagina's op één A4'tje afdrukt. Zo bespaar je heel wat papier;
- druk enkel in kleur af als het echt nodig is. Recto-verso en zwart-wit afdrukken zijn standaard instellingen, maar je kan deze instellingen voor een bepaalde printopdracht steeds wijzigen;
- druk van een groter document enkel die pagina's af die je echt nodig hebt.

c) Kopiëren

Neem ook zo weinig mogelijk kopieën.

Als je toch moet kopiëren, hanteer dan volgende principes:

- kopieer zoveel mogelijk recto verso;
- kopieer niet in kleur, tenzij je het echt nodig hebt. Recto-verso en zwart-wit zijn standaard instellingen, maar je kan deze instellingen voor een bepaalde kopieeropdracht steeds wijzigen;
- controleer alle instellingen voor je kopieert en kopieer niet meer dan je nodig hebt;
- verklein zoveel mogelijk: twee A5'jes passen precies naast elkaar op één A4-blad.

Bedenk dat scannen maar evenveel tijd vergt als kopiëren.

LAPTOP EN PC

- Indien u over een laptop van de werkgever beschikt, kan u deze laptop ook aanwenden voor telewerk of beperkt thuisgebruik.
- Mochten er problemen zijn met de laptop, zal de ICT dienst de oorspronkelijke configuratie op de laptop terugplaatsen. Dit zal steeds gepaard gaan met verlies van persoonlijke instellingen en persoonlijke data op de harde schijf van de laptop.
- Indien voor de goede uitoefening van uw job een laptop noodzakelijk is, kan u deze aanvragen via een mail naar het diensthoofd ICT met grondige argumenten en advies van uw leidinggevende. De ICT dienst beoordeelt de vraag, kadert ze in het ICT beleid van de organisatie en bespreekt ze met de algemeen directeur.

MAILEN

Het e-mailadres dat de organisatie u ter beschikking stelt, wordt voor professionele doeleinden gebruikt. Het versturen en ontvangen van persoonlijke e-mails tijdens de kantooruren zorgt voor een vermindering van de reëel geleverde prestaties en een vermindering van de kwaliteit van de dienstverlening. Het gebruik van e-mail is dan ook enkel toegestaan voor professionele doeleinden.

Het feit dat het e-mailadres de persoonlijke naam bevat, betekent niet dat alle e-mail een persoonlijk karakter krijgt. Het is altijd mogelijk dat een medewerker van de ICT dienst in het kader van zijn functie kennis moeten nemen van (delen van) deze gegevens.

E-mailen namens het bestuur

E-mail gebruikt u om in naam van het lokaal bestuur Beveren te communiceren. Een e-mail is informeler dan een brief. Toch is het belangrijk taalkundig correct en klantvriendelijk te blijven.

Het is niet toegelaten de privé email (zoals hotmail, gmail, telenet.be,...) te gebruiken voor professionele communicatie.

Je emailhandtekening wordt gegenereerd door de dienst informatica.

Voorbeeld autohandtekening:

Met vriendelijke groeten

KELLY SMET
Beleidsmedewerker •
BEVEREN VERBINDT
Stationsstraat 2 • 9120 Beveren
tel 03 750 46 14 • gsm 0486 70 12 07
www.beveren.be • Facebook • Twitter • Disclaimer

Het gebruik van vermeldingen zoals “bezoek www.beveren.be en schrijf je in op de elektronische nieuwsbrief!” of “Denk aan het milieu of “Druk dit bericht niet onnodig af” is niet toegestaan.

De regels van de huisstijlgids zijn toepasbaar op e-mailberichten. We gebruiken zo bijvoorbeeld steeds lettertype Source Sans Pro in een zwarte kleur.

Officiële aanvragen

Burgers, bedrijven, … gebruiken e-mail meer en meer om aanvragen aan het bestuur over te maken. Mails met aanvragen waarin het college van burgemeester en schepenen een beslissing moet nemen, moeten dan ook geregistreerd worden door het KCC (zoals briefwisseling). U doet dit door de mail door te sturen naar postregistratie@beveren.be . U handelt de mail verder via het postregistratiesysteem af. Het formele antwoord op de aanvraag met de beslissing van het college bezorgt u via de klassieke briefwisseling en/of via het postregistratiesysteem.

Zelf mailen

Gebruik nooit het e-mailadres van een ander personeelslid. Dit is verboden.
Een persoonlijk e-mailadres is strikt persoonlijk. Het is ook niet toegelaten de handtekening of het reply-adres te wijzigen opdat geadresseerde zou denken dat hij een e-mail van een andere persoon ontvangt.

Wanneer e-mail gebruiken?

- Gebruik e-mail voor eenvoudige, niet-dringende berichten:
  om vragen te beantwoorden, om vragen te stellen die niet onmiddellijk beantwoord moeten worden, om informatie aan te vragen, om een taak te verdelen, om afspraken te bevestigen.
- Verzwaar een mail niet onnodig met beeldmateriaal.
- Verspreid geen vertrouwelijke gegevens van het bestuur, personeelsleden of andere partijen waarmee u in de uitvoering van uw taak in contact komt, tenzij dit noodzakelijk is voor de goede uitvoering van uw werk.

Aan wie?

- Richt u in het veld ‘aan’ aan de persoon waarvan u een antwoord of reactie verwacht.
- Richt u in het veld “cc” aan de perso(o)n(en) van wie u geen antwoord of reactie verwacht, maar die wel op de hoogte moeten zijn van de zaak.
  Plaats niet automatisch uw diensthoofd of collega’s in “cc”. Denk goed na alvorens een hele lijst mensen een kopie te bezorgen van uw mail. Denk aan de tijd die het vraagt van die mensen om deze mail te lezen.
- Gebruik het veld “bcc” slechts uitzonderlijk (bijvoorbeeld bij een prijsvraag naar externe leveranciers). Wij zijn een open organisatie.
- Mails aan grote groepen of “iedereen” zijn verboden, tenzij absoluut noodzakelijk. Indien noodzakelijk, vraagt u voorafgaandelijk toestemming aan de algemeen directeur.

- Indien u nodeloos een mail krijgt, laat dat dan weten.

Goed gebruik mail en mailbox

- Controleer uw mailbox minstens dagelijks. Geef binnen de 2 werkdagen het nodige gevolg aan binnenkomende berichten of geef feedback aan de afzender wanneer deze een antwoord kan verwachten. Ken aan de afwikkeling van e-mailberichten dezelfde prioriteit toe dan aan de andere communicatiekanalen (brieven, faxen, …)
- Abonneer u alleen op professioneel relevante elektronische magazines (E-zines of mailinglijsten).
- Hou uw inbox leeg!
  Creëer subfolders om uw mails in te bewaren.
  Beperk de grootte van uw totale mailbox tot maximaal 1 gigabyte.
  Let vooral op de bijlagen (foto's, word-documenten, PowerPoint presentaties, …). Vergeet niet regelmatig de "verzonden items" te deleten (kan ook automatisch via instellingen).
- Indien u het lokaal bestuur verlaat zal uw bestaande persoonlijke brievenbus in overleg zo snel mogelijk worden gesupprimeerd. U dient uiteraard zelf een afwezigheidsassistent in te stellen (met doorverwijzing naar het contactadres van collega's).
- Zet de vraag naar een leesbevestiging standaard af en gebruik dit nooit voor intern mailverkeer. Enkel in specifieke gevallen (bv. afspraken rond belangrijke dossiers met externen, mails die vasthangen aan bepaalde termijnen) kan het vragen naar een leesbevestiging wel.

Goed gebruik dienstmailadres & dienstmailbox

- Naast de eigen mailbox, beschikt u ook over een gezamenlijk dienstmailadres met bijhorende gezamenlijke dienst inbox.
  Bovenstaande richtlijnen gelden uiteraard ook voor deze dienstmailbox!
- Het diensthoofd organiseert het gebruik van de dienstmailbox en bepaalt wie verantwoordelijk is voor de afhandeling van de mails in de dienstmailbox.

Meer richtlijnen hierrond vind je terug in het huisstijlhandboek op het intranet.

Bijlagen in mails

- Eventuele bijlagen aan e-mailberichten kunnen enkel worden opgemaakt met de standaardsoftware die aan het personeelslid ter beschikking is gesteld.
- Wanneer derden u bijlagen toesturen die u niet kan openen met de standaardsoftware, vraag dan voorafgaandelijk toestemming aan dienst ICT om software te downloaden en/of te gebruiken die toelaat de bijlagen te consulteren. Desgevallend zal de ICT dienst zelf overgaan tot het openen van de bestanden en deze in een andere vorm (vb. uitgeprint document) aan u overmaken.
- Met het oog op het voorkomen van overbelasting van de systemen, mogen de mails die u verstuurt maximaal 8 MB groot zijn.
  Indien u toch een bestand moet verzenden dat groter is dan 8 MB kan u dit doen via de website www.wetransfer.com . Via deze weg kan u gratis grote bestanden bezorgen zonder enige registratie. Per transfer kunnen maximum 20 personen aangeschreven worden. De bestanden blijven 2 weken op de site beschikbaar. Biedt www.wetransfer.com niet voldoende mogelijkheden, dan kan via de ICT dienst gekeken worden naar mogelijke alternatieven.

Er staat ook een beperking op de grootte van binnenkomende mails.
Ook deze mogen slechts 8 MB groot zijn.

MELDINGEN

Zie topdesk

NETWERK

- U dient uw gegevens die werkgever gerelateerd zijn enkel op het netwerk op te slaan (L-schijf) en niet op **lokale** middelen zoals de C-schijf of **mobiele gegevensdragers** (vb. USB stick). Mobiele gegevensdragers gebruik je om tijdelijk een kopie van een document op te slaan. Op het netwerk kunt u rekenen op een meervoudige beveiliging van de bestanden (back ups). Op notebooks en mobiele gegevensdragers worden geen backups genomen.
- Gegegevens van het bestuur mogen niet op eigen initiatief "in the cloud" worden opgeslagen, bijvoorbeeld via een persoonlijke dropbox, google-drive of dergelijke.
- **Structuur van de netwerkmappen.**
  Elke dienst heeft zijn eigen dienstmap op het netwerk (vb: L:kwaliteit en beleid). Deze is enkel toegankelijk (via rechten) door de medewerkers van de betrokken dienst en de hiërarchische lijn (afdelingshoofd, algemeen directeur). De medewerkers van de ICT dienst hebben omwille van praktische technische redenen toegang tot alle mappen.
  De mappenstructuur onder de dienstmap wordt gevormd op basis van de kernprocessen van de dienst. Alle medewerkers hebben toegang tot deze mappen. Zoveel mogelijk documenten moeten centraal in deze mappen opgeslagen worden.
  Onder elke dienstmap is voor elke medewerker van de dienst een persoonlijke map beschikbaar, waartoe alleen zij toegang hebben. In uw persoonlijke map bewaart u geen dienstdossiers, maar wel bijvoorbeeld uw voorbereiding voor het functioneringsgesprek met uw diensthoofd.
  De L:schijf bevat een map "**samenwerking**". Via deze map kan u grote bestanden uitwisselen. U kan er tijdelijk documenten plaatsen die medewerkers van een andere dienst willen consulteren.
  Let op: u dient de bestanden op de eigen publieke map regelmatig zelf te verwijderen.
- **BELANGRIJK: houd uw dienstmappen net en ordelijk!**
  Wees zuinig met de beschikbare ruimte!
  U bent mee verantwoordelijk voor de goede werking van het netwerk. Spring dus zuinig om met de beschikbare schijfruimte. Verwijder overbodige bestanden of bestanden die meermaals voorkomen op het netwerk. Schoon uw digitaal dossiermapje bij het sluiten van het dossier. Denk hierbij aan het verwijderen van verschillende versies van een document in de ontwerpfase, foto's uit diverse hoeken van een item terwijl u toch maar één foto echt kan gebruiken, internetafbeeldingen die u nodig had voor een PowerPointpresentatie, …
- **Archivering**
  Niet frequent gebruikte bestanden (die bewaard moeten worden) kunnen in samenspraak met de ICT dienst en archief digitaal gearchiveerd worden.
- **Privaat**
  Het opslaan van privé-gerelateerde informatie op de harde schijf van het werkstation of op een andere opslagruimte is verboden.
- **Intranet**
  Het lokaal bestuur beschikt over een intranet. Dit is terug te vinden via: http://intranet.beveren.be/. Via deze website kan een wachtwoord aangevraagd worden. Op het intranet vindt u allerlei nuttige documenten en richtlijnen terug zoals het arbeidsregelement, telefoonlijst, huisstijlgids,…

SOCIALE MEDIA

Sociale netwerksites zoals Facebook, Twitter, LinkedIn, … kennen een immens succes. Het gebruikersaantal blijft groeien alsook de impact van het medium.

Ook voor het lokaal bestuur zijn sociale media belangrijke communicatiemiddelen. Daarom krijgen medewerkers toegang tot deze kanalen. We rekenen er dan ook op dat iedereen efficiënt met dit middel omspringt.

Bij het gebruik van sociale media wordt de communicatie voor een groot stuk losgelaten. Het is daarom belangrijk dat men onderstaande richtlijnen goed opvolgt. Op deze manier worden onze personeelsleden de perfecte ambassadeurs van onze organisatie.

Als u het lokaal bestuur vertegenwoordigt op sociale media, volg dan deze richtlijnen:

- **Overleg**
  Opstarten van nieuwe kanalen, profielen en accounts gebeurt na overleg met de communicatiedienst en enkel en alleen na goedkeuring van deze dienst.
- **Maak je kenbaar, maak bewaak hierbij je privacy**
  Iedereen die op sociale media communiceert vanuit zijn werk of in zijn vrije tijd over de organisatie praat, moet duidelijk maken vanuit welke rol hij of zij dat doet. Alleen de communicatiedienst kan uit naam van de gemeente spreken. De anderen doen dit enkel vanuit de eigen naam. Bewaak je eigen privacy en geef niet onnodig je gegevens door.
- **Wees eerlijk en geloofwaardig**
  Bij communicatie op sociale media communiceer je in een sociale omgeving. Berichten en reacties kunnen andere gebruikers positief en negatief raken. Bij het converseren voor of over het werk moet het gedrag op sociale media overeenstemmen met het normale gedrag op het werk.
- **Wees voorzichtig**
  Breng geen gevoelige of vertrouwelijke informatie naar buiten. Geef geen info vrij en doe geen toezeggingen zonder dat u daartoe bevoegd bent. Blijf binnen de wettelijke kaders van het auteursrecht. Laat officiële mededelingen of contacten met de pers altijd via de communicatiedienst verlopen.
- **Blijf positief**
  Schrijft u iets over de gemeente, doe dit dan in positieve zin. Hebt u opmerkingen, suggesties of klachten over de werking van onze organisatie? Gooi die dan niet op het internet, maar spreek er uw leidinggevende over aan. Onthoud u van beledigende uitspraken en rond af als de toon negatief wordt.
- **Luister en vraag raad**
  Deel uw expertise en laat merken dat u luistert. Merkt u dat iemand zich negatief uitlaat over de gemeente of haar dienstverlening? Breng de dienst communicatie dan op de hoogte via mail aan communicatie@beveren.be. Ook als u twijfelt of u zelf de geschikte persoon bent om te reageren, speelt u de bal beter door aan uw diensthoofd of de communicatiedienst.
- **Reageer snel**
  Social media zijn bij uitstek een vlug medium. Reageer, net zoals bij e-mail, binnen de 2 werkdagen op vragen, opmerkingen, suggesties … Het is niet altijd nodig om meteen te reageren op berichten of reacties van anderen. Het is dikwijls aangewezen om de conversatie te laten gebeuren en pas in te grijpen als het verkeerd dreigt te gaan. Als mensen persoonlijk worden of als er conclusies of emoties komen aan de hand van foutieve of emotionele informatie, kan u ingrijpen om een conversatie weer in de positieve richting te sturen.
- **Surf met mate**
  Uiteraard vertoeft u tijdens de werkuren enkel op social media sites binnen een werkgerelateerde contex.

SOFTWARE

- U mag absoluut zelf geen programma's op een ICT-middel installeren tenzij mits uitdrukkelijke toestemming van de ICT dienst. In alle andere gevallen doen de medewerkers van de ICT dienst dit voor u.
- U mag geen programma's opstarten die de ICT dienst niet heeft goedgekeurd of aangeboden (geen free- of shareware, niet-legale software, spelprogramma's, …)
- Indien u als personeel toegang wenst tot een softwarepakket waarover de werkgever beschikt, kan u dit via Topdesk aanvragen.
- Aanbeveling: gelieve geen foto te installeren als screensaver/achtergrond bureaublad. De hoge resolutie, vaak noodzakelijk om het beeld duidelijk weer te geven, zorgt voor belasting van het netwerk en vertragingen.

TELEFONIE

Ook gebruik van een vaste telefoon of een gsm, smartphone,… valt onder de noemer elektronische communicatiemiddelen en is dus ook onderwerp van deze gedragscode. Zie ook rubriek “eigenlijk en oneigenlijk gebruik”.

Vaste telefoon

- U kan andere personeelsleden en diensten intern bereiken via verkorte nummering: u draait enkel de 4 laatste cijfers van het telefoonnummer.
  (vb: infodienst: 15 80)
- Het overzicht van de (verkorte) nummers van de collega’s kan u terugvinden in Topdesk .
- Om een persoon buiten het telefoonnetwerk te bereiken draait u steeds eerst “0” voor een buitenlijn, gevolgd door het nummer.
  (vb: 0 03 775 70 54 voor de bib van Haasdonk)
- U kan vrij telefoonnummers in België bereiken. Slechts enkele personeelsleden hebben de mogelijkheid om binnen de Benelux te bellen.
  Mocht u willen telefoneren naar het buitenland, neem dan contact met de mensen van het onthaal die de algemene telefooncentrale bedienen. Zij zullen het buitenlandse nummer draaien en u doorverbinden.
  (gemeente: 03 750 15 11 – OCMW: 03 750 46 00).
- 0800 nummers en noodnummers zijn door iedereen bereikbaar.
  077 en 090 nummers zijn nooit bereikbaar.

Mobiel bellen

Medewerkers met een bepaalde jobinhoud of functie en die vaak van hun vaste werkplek weg zijn, krijgen een mobiel toestel met abonnement ter beschikking om de werkefficiëntie en bereikbaarheid te verhogen. Een aparte ‘personeelsnota mobiel bellen’ beschrijft de geldende afspraken, de soorten mobiele toestellen, de toewijzing, de aanvraagprocedure, de afrekening en de verzekering. Deze nota vindt u terug op het intranet.

De medewerker verbindt zich ertoe het ter beschikking gestelde toestel te gebruiken als een goede huisvader. Van zodra een SIM-kaart ter beschikking wordt gesteld door het bestuur, wordt het mobiele toestel opgenomen in de beheertool en de telefoonboek.

Telefoonetiquette

De telefoon is een belangrijk communicatiemiddel. Ondanks de opkomst van e-mailverkeer verlopen nog steeds heel wat belangrijke gesprekken via de telefoon. We spenderen nog steeds enorm veel tijd aan de telefoon: door klanten of partners te woord te staan of hen naar de juiste persoon door te schakelen, …
Een goede telefoonetiquette is onontbeerlijk voor een klantvriendelijke organisatie. Samengevat: bedien de ander met waardevolle aandacht.

11 telefoontips voor klantgericht telefoneren

1) Laat je telefoon niet meer dan drie keer rinkelen en zorg voor een glimlach in de stem. Spreek niet te luid en niet te stil.
2) Maak een klantgerichte opening:
   Goedemorgen/-middag/-avond
   gemeente Beveren – dienst X (bedrijfsnaam)
   (u spreekt) met (eigen naam)
3) Spreek rustig, articuleer goed en laat in uw intonatie onder andere doorklinken dat de beller bij u welkom is.
4) Laat iemand niet onnodig lang wachten: de irritatiegrens ligt bij zo'n 25-30 seconden.
5) Licht regelmatig beeldend toe wat u aan het doen bent; tijdens het telefoneren ziet de ander u niet.

6) Wees klantgericht, dus luister vaardig en actief:
   - Laat iemand spreken / uitpraten
   (u heeft 2 oren en maar 1 mond, gebruik ze telefonerend in deze verhouding)
   - Laat onder andere een "ja", "jazeker" en "hum" regelmatig horen
   - Vat informatie en/of boodschappen kort samen + laat dit bevestigen met een "ja"
   - Vraag klantgericht door waar nodig
7) Verbind warm door:
   Als je een correspondent doorverbindt met een collega, zorg er dan voor dat beiden voor hun telefoongesprek weten met wie ze zullen spreken. Vermeld eventueel bijkomende gegevens (functie, organisatie, dossier waarover het gaat) om de informatie zo volledig mogelijk te maken. Alle informatie die de klant al gegeven heeft, wordt doorgeven aan de collega vooraleer we de lijn doorschakelen. Op die manier hoeft de klant zijn verhaal niet meerdere keren opnieuw te doen (en heeft hij niet het gevoel dat hij van het kastje naar de muur gestuurd wordt).
8) Wees pro-actief:
   Bij afwezigheid van de gevraagde persoon, vraag dan of u iets kunt doen. Noteer de beller zijn of haar contactgegevens en diens vraag. Bezorg deze informatie zo snel mogelijk aan je collega.
9) Kan u de klant niet onmiddellijk helpen, vertel hem/haar dat u eerst op zoek gaat naar de nodige informatie en dat u hem/haar later zal terugbellen. Noteer zorgvuldig zijn/haar naam, telefoonnummer en de benodigde informatie. Hou u ook aan deze belofte.
10) Vat aan het einde de gemaakte afspraken klantgericht kort samen en laat dit klantgericht bevestigen.
11) Sluit steeds het telefoongesprek beleefd af. Bijvoorbeeld: "Graag gedaan, goedenavond meneer/mevrouw". Let erop dat de klant geen vragen meer heeft op het einde. U kan voor de zekerheid wachten totdat de beller zelf inhaakt.

Schakel bij afwezigheid het telefoontoestel door naar een andere collega of de balie. Verwittig de collega's eerst van deze doorschakeling.

TOPDESK

De dienst informatica werd in het verleden vaak overstelpt met telefoons en/of enthousiaste collega's die terplaatse hun ICT probleem kwamen melden. Hierdoor werden de ICT medewerkers vaak (onnodig) gestoord tijdens hun werkzaamheden. Om dit probleem op te lossen heeft de dienst Topdesk in gebruik genomen. Dit is een helpdeskprogramma voor meldingen, klachten, … gerelateerd aan ICT diensten.
Uw melding(en) worden geregistreerd en behandeld door een ICT medewerker.
Wanneer u een melding doorgeeft via Topdesk, ontvangt u een ticketnummertje. Meldingen met een ticketnummer worden sneller behandeld dan meldingen zonder ticketnummer (principe: no ticket, no service). Een gebruikershandleiding van Topdesk is beschikbaar via intranet.

Hoe een melding in Topdesk aanmaken?

1. **Topdesk selfservice desk:**
   Meldingen komen rechtstreeks terecht bij de medewerkers van de helpdesk ICT.
   Elke melding die u maakt krijgt een ticketnummer, prioriteit en behandelaar toegewezen.
   Meldingen met een ticketnummer worden met voorrang behandeld ten opzicht van meldingen zonder ticketnummer.
2. **E-mail:**
   Om meldingen aan te maken via e-mail moet u mailen naar helpdeskict@beveren.be .
   Deze mail wordt behandeld en geïmporteerd in Topdesk. Ook hier krijgt u een ticketnummer, prioriteit en behandelaar toegewezen.
   Mails verzonden naar een persoonlijk e-mailadres van een medewerker van ICT worden niet prioritair behandeld.

In dat geval zal u een vriendelijk mailtje ontvangen met het verzoek om de melding in te geven via Topdesk of door te sturen naar helpdeskict@beveren.be .

3. **Telefoon:**
   Telefonische meldingen mogen enkel nog gemaakt worden in het geval Topdesk of de mail niet meer beschikbaar is (netwerkproblemen, internetproblemen, mailproblemen,…).
   Indien een collega op de dienst wel Topdesk kan opstarten kan u alsnog via die collega zijn toestel de melding laten ingeven.
   Meldingen via Topdesk worden normaliter sneller geregistreerd en toegewezen.
   Het algemene helpdesknummer voor ICT is **03 750 16 80.**
   Oproepen die gedaan worden op het persoonlijk nummer van een medewerker worden in de regel door het algemene helpdesknummer opgenomen tenzij de medewerker wel direct wenst op te nemen.
4. **Mondeling:**
   Er worden geen notities meer genomen van meldingen die mondeling worden doorgegeven tenzij de urgentie dit rechtvaardigt.
   U zal vriendelijk verzocht worden om bij voorkeur methode 1 of 2 te gebruiken indien niet urgent.

Andere functionaliteiten in Topdesk

In Topdesk kan u niet enkel meldingen aanmaken, maar ook reserveringen maken (ICT materiaal , vergaderzalen, dienstvoertuigen, laptops, ...), het kennissysteem raadplegen, telefoonnummers opzoeken, …

VIRUSSEN EN SPAM

Het lokaal bestuur Beveren wil de verspreiding van en besmetting door computervirussen tegengaan. Op 3 niveaus worden beschermende maatregelen (SPAM filters) genomen: bij provider Proximus, op serverniveau en lokaal op de werkstations. Toch kan het nog steeds voorvallen dat inventieve snoodaards erin slagen om door te dringen tot in het hart van onze IT-architectuur.
Neem dan ook zelf volgende regels in acht:

- Delete berichten met spam en mogelijke virussen onmiddellijk. Neem bij twijfel (anderstalige berichten, berichten van onbekende personen, abnormale werking van het systeem, …) steeds contact op met de ICT dienst.
- Op elke computer of laptop moet de antivirussoftware die door de ICT dienst ter beschikking wordt gesteld, steeds geactiveerd zijn.
- Wanneer u regelmatig van eenzelfde onbekende afzender niet-professionele berichten ontvangt, dient u de afzender per kerende te verzoeken om geen dergelijke correspondentie meer te versturen. Op uw verzoek of wanneer de ICT dienst ontdekt dat één bepaalde afzender regelmatig niet-professionele berichten verstuurt, kan het bestuur beslissen dat berichten van deze afzender worden geblokkeerd, zodat geen berichten meer kunnen worden ontvangen door de afzender.

U verstuurt zelf geen berichten die als een aantasting van de menselijke waardigheid kunnen worden beschouwd, bijvoorbeeld berichten die door de bestemmeling kunnen worden ervaren als racistisch, discriminerend (op basis van geslacht, seksuele geaardheid, godsdienst, afkomst, handicap, …) of seksueel intimiderend.

WACHTWOORDEN

Zie beveiliging

Akkoordverklaring

IK ERKEN EEN EXEMPLAAR TE HEBBEN ONTVANGEN VAN DEZE GEDRAGSCODE MET BIJLAGEN EN VERKLAAR VAN DE INHOUD ERVAN KENNIS TE HEBBEN GENOMEN.

IK VERKLAAR DAT IK DE INHOUD BEGRIJP, VERKLAAR MIJ ERMEE AKKOORD EN VERBIND MIJ ERTOE DEZE TE ZULLEN NALEVEN.

{Naam}
{Plaats en datum}

Voor akkoord,
{Handtekening}