Hoofdstuk 1 : Gebruik van ICT middelen

1.1. Draagwijdte en toepassingsgebied

Dit beleid regelt de toegang, het intern en extern gebruik en de controle van de ICT-infrastructuur die door de organisatie ter beschikking wordt gesteld van de medewerker, evenals de van thuis uit meegebrachte infrastructuur.
Dit beleid geldt eveneens voor alle gegevens die via deze systemen worden geproduceerd, overgedragen of erin worden opgeslagen.
De ter beschikking gestelde ICT-middelen, alsook de informatie op het systeem, zijn en blijven eigendom van de organisatie. Onder ICT-middelen wordt begrepen: telefonie, smartphones, laptops, pc's , harde schijven, usb-sticks, tablets, printers,…

1.2. Verantwoordelijkheden van de gebruiker

Het lokaal bestuur doet een beroep op het gezond verstand van z'n medewerkers bij het gebruik van de ICT-middelen die ter beschikking gesteld worden. Als gebruiker draag je zorg voor deze ICT-infrastructuur. Je wordt als medewerker geacht je computer, het netwerk, internet, email, en telefoon te gebruiken om de kwaliteit van het werk te bevorderen zonder het imago van de organisatie te schaden. Het gebruik moet dus ten dienste staan van het lokaal bestuur en haar doeleinden.
Ongeoorloofd gebruik is ruimer dan illegaal gebruik en omvat ook het gebruik van e-mail en internet voor privaat of commerciële doeleinden of een gebruik dat de infrastructuur kan overbelasten.
Indien het lokaal bestuur privé gebruik toestaat, gaat het niet om een recht, maar wel om een gunst die steeds kan worden beperkt of ingetrokken worden.
De gebruiker heeft, voor zover van toepassing, een aantal verantwoordelijkheden en plichten die hieronder, niet limitatief, opgesomd worden:

1.2.1 Algemeen

- Het in goede toestand bewaren van de ICT-middelen die ter beschikking gesteld werden.
- Niet onbeheerd achterlaten van de ter beschikking gestelde ICT-middelen en het nemen van voldoende veiligheidsmaatregelen om diefstal ervan te verhinderen. Bij diefstal moet de ICT-dienst zo snel mogelijk gecontacteerd worden.
- Nemen van voldoende veiligheidsmaatregelen die de mogelijkheid tot het inbreken op de systemen van de organisatie en diefstal van informatie zo klein mogelijk maakt.
- Nooit meedelen van een gebruikersnaam en wachtwoord aan derden (zoals b.v. collega's, de helpdesk, jobstudenten, stagiairs, consulenten, externen, via e-mail, op onbekende websites en locaties, …). Iedere gebruiker is verantwoordelijk en aansprakelijk voor alles wat onder zijn/haar loginnaam en wachtwoord gebeurt.
- Het afsluiten van de werkplek bij het verlaten voor een bepaalde periode wanneer men de laatste aanwezige op de werkplek is.
- Het activeren van de schermbeveiliging van de PC en andere ICT middelen. Dit kan heel eenvoudig door gelijktijdig de "Windows-toets" + "L" in te drukken.
- Het beveiligen van alle ICT-middelen die op het netwerk verbonden worden en alle vertrouwelijke en bedrijfsgevoelige informatie die op deze ICT-middelen bewaard worden (door bv. een opstartwachtwoord, een pincode, een schermbeveiliging, … te voorzien).

1.2.2. Netwerk

Toegang tot de computerinfrastructuur en het netwerk wordt verleend door individuele authenticatie. Het gaat hier in principe om een gebruikersnaam en wachtwoord. Meer informatie over wachtwoorden, vind je in het wachtwoordenbeleid.
Op het netwerk zijn een aantal netwerkschijven aanwezig; elk met zijn eigen specifieke doeleinden. Door medewerkers aangemaakte bestanden moeten steeds bewaard worden op de daartoe voorziene netwerkschijf en NIET op de lokale harde schijf.
Iedere gebruiker is mede verantwoordelijk voor de goede werking van het netwerk. De medewerkers worden gevraagd om zuinig om te springen met de schrijfruimte op de servers. Overbodige bestanden dienen regelmatig verwijderd te worden.
Bestanden krijgen een duidelijke naam en worden opgeslagen in de juiste dienstmappen zodat de toegankelijk tot documenten bij andere interne personen steeds verzekerd is. Het is niet toegelaten om bestanden op te slaan buiten het administratief netwerk (vb. Dropbox, Google Drive, …)

1.2.3. Internet

Elk bezoek van websites met een duidelijke link naar het werkkader is binnen de werkuren toegestaan, voor zover:

- de opgezochte informatie een relevante meerwaarde biedt aan de goede uitvoering van de opgelegde taken
- slechts voor een tijdspanne die in redelijke verhouding staat tot het nut ervan voor de uitvoering van de taken.
- surfen op internet houdt risico's in en de kans op een aanval via bepaalde sites is realistisch. De medewerker moet:
    - steeds bewust zijn dat hij/zij de organisatie vertegenwoordigt op internet. Veel websites houden een spoor bij van bezoek en kunnen soms de herkomst en de elektronische identiteit vaststellen van de persoon en van de organisatie;
    - de configuratie van de webbrowser en de beveiligingssoftware (antivirus, antispam, firewall) zoals ingesteld door de organisatie ongewijzigd houden;
    - niet-professionele sites verlaten bij vermoeden dat de bezochte site niet is waar naar gezocht werd.
- bij het downloaden van bestanden beperkt de medewerker zich tot het strikt noodzakelijke in het kader van zijn beroepsactiviteiten, voor zover de organisatie het downloaden toestaat;

Het internetgebruik voor persoonlijke doeleinden is als gunst toegestaan buiten de werkuren (tijdens middagpauze).
Voor het persoonlijk gebruik dienen de onderstaande gedragsregels op dezelfde manier gehanteerd te worden alsof het zou gaan om professioneel gebruik. Het persoonlijk gebruik mag geenszins de goede werking van het computernetwerk of de productiviteit van de medewerker benadelen.

1.2.4. E-mail

De officiële e-mailadressen toegekend door de ICT verantwoordelijke mogen onbeperkt gebruikt worden voor de uitvoering van de arbeidstaak voor zover:

- de uitgewisselde informatie ondubbelzinnig gelinkt is aan de opgelegde taken;
- in de e-mail geen vertrouwelijke informatie wordt meegedeeld waartoe de medewerker geen bevoegdheid heeft om deze mede te delen;
- de geldende strafregels worden nageleefd.
- De verzender van een e-mail is verantwoordelijk voor de inhoud van dit bericht.
- Het gebruik van e-mail en online communicatiemiddelen dient te gebeuren in overeenstemming met de aanbevelingen inzake de bescherming van de persoonlijke

levenssfeer. Dus mogen er geen persoonsgegevens zonder afdoende veiligheidsmechanismen via e-mail en online communicatie middelen worden overgemaakt. Alvorens gevoelige bestanden via e-mail en online communicatiemiddelen te versturen, dient de medewerker ervoor te zorgen dat deze bestanden goed vercijferd zijn. Een bijlage waarin de persoonsgegevens staan zal toegevoegd worden aan de e-mail, beveiligd met een wachtwoord. Dit wachtwoord zal op een andere manier verstuurd worden naar de ontvanger of ten minste via een andere e-mail met enkel het wachtwoord.

- Bij langdurige afwezigheid van de medewerker (meerdere dagen) dient een automatisch antwoord ingesteld te worden zodat correspondenten op de hoogte zijn van de langdurige afwezigheid ("out of office").
- De medewerker zal geen e-mails naar grote groepen medewerkers versturen ("To All Users"). Grote bestanden worden bij voorkeur op het interne documentbeheersysteem van de organisatie geplaatst. De e-mail bevat enkel een link naar de bestanden.
- het personeelslid heeft geen controle over e-mails die hem/haar worden toegestuurd en kan hiervoor dan ook niet aansprakelijk worden gesteld. Het personeelslid wordt evenwel verondersteld dergelijke e-mails na ontvangst dadelijk te verwijderen en geenszins naar anderen door te sturen. Het personeelslid dat van bepaalde afzenders op regelmatige basis dergelijke e-mails krijgt opgestuurd, dient deze afzender zonder verwijl te verzoeken het toesturen van deze e-mails stop te zetten. Indien dergelijk e-mailbericht onderaan een mogelijkheid voorziet om uit te schrijven (vooral bij mailinglijsten waarvoor men zich vrijwillig inschrijft), dient via deze weg de schrapping gevraagd te worden;

Alle uitgaande e-mailberichten worden afgesloten met enerzijds een handtekening die beantwoordt aan de huisstijl en anderzijds de hieronder vermelde 'disclaimer'.
“De informatie in deze e-mail is vertrouwelijk en uitsluitend bedoeld voor gebruik door de geadresseerde. Als U deze e-mail per vergissing heeft ontvangen, gelieve hem dan met de toegevoegde bestanden te vernietigen.”
“Les informations contenues dans cet e-mail sont confidentielles et destinées uniquement au destinataire. Si vous avez reçu cet e-mail par erreur, détruisez-le avec les fichiers ajoutés.”
Het ter beschikking gestelde e-mailadres mag niet voor persoonlijke doeleinden gebruikt worden.

Correct gebruik van Aan, CC, BCC in e-mails

Het is belangrijk dat we een onderscheid maken tussen de velden waar je de bestemmelingen van een e-mail invult. Hieronder vind je een richtlijn over welk veld wanneer in te vullen.

“Aan”

Je zet je bestemmelingen van je e-mail in het “Aan” veld als je van deze mensen een actie verwacht. De persoon of kleine groep personen maken deel uit van de mensen waarvan jij iets verwacht. Deze personen of persoon zien elkaars e-mailadres. Zij kunnen mekaar dus ook mailen. Je zal dit doen als je bv. gezamenlijk aan een project werkt. **Zet dus nooit meerdere privé e-mailadressen in het "Aan" veld, gebruik hiervoor het BCC veld!**

“CC” Carbon Copy.

De personen of kleine groep mensen die je in CC zet, krijgen een kopie van je e-mail. Er wordt niet direct actie verwacht maar je wil deze kleine groep laten weten dat er een e-mail gestuurd werd. Belangrijk: zowel bestemmelingen ingevuld in “Aan” als in “CC” zijn een zeer kleine groep van mensen. Als je een grote groep van mensen een e-mail wilt zenden, gebruik je standaard “BCC”.

“BCC” Blind Carbon Copy.

De personen die je hier invult weten van elkaar niet dat zij dezelfde e-mail kregen. Dat is belangrijk om weten. Je zal “BCC” gebruiken als de groep van mensen groot is (vanaf 15 mensen, als je niet gezamenlijk aan een project werkt). “BCC” zal je ook gebruiken om de privacy van de ontvangers te beschermen als je een groep mensen een e-mail stuurt. Je voorkomt hier tevens mee dat als iemand een e-mail per vergissing antwoord met “allen beantwoorden” de vele bestemmelingen een (overbodige) e-mail verstuurt. Een ander voordeel is het kleiner risico op spam. Niemand kan de lijst met e-mailadressen gebruiken in een spambericht.

1.2.5. Verwijderbare media

Onder verwijderbare media cd-roms, USB sticks, verwijderbare (externe) schijven, tapes, geheugenkaartjes,…

- Er mag enkel verwijderbare media gebruikt worden die wordt uitgeleend door de ICT dienst. Persoonlijke verwijderbare media mogen niet gebruikt worden. Het vaste netwerk moet zodanig beveiligd zijn dat het aansluiten van ongeoorloofde apparatuur opgespoord of verhinderd kan worden.
- Alle verwijderbare media zijn versleuteld
- Ingeleverde media worden na teruggave gewist

1.2.6. De veiligheid van gegevens

- Apparaten en media mogen niet onbeheerd achtergelaten worden in openbare ruimten.
- Het meenemen van informatie buiten de gebouwen van het Lokaal Bestuur kan enkel als dit noodzakelijk is voor de uitoefening van de functie en steeds onder toezicht van een bevoegd persoon.
- Verstuur documenten/pakjes steeds naar de specifieke dienst/persoon voor wie ze bedoeld zijn.
- Voor elk transport van medische persoonsgegevens buiten het Lokaal Bestuur moeten transportgegevens (wie, wat, wanneer) geregistreerd worden. Zorg ervoor dat de persoonsgegevens niet zichtbaar zijn voor onbevoegden en dat de gegevens of bv geneesmiddelen in een verzegelde verpakking of container zitten wanneer ze opgehaald worden door een externe transporteur.
- Bij uitwisseling van persoonsgegevens is een wederzijdse authenticatie noodzakelijk. De transmissie van vertrouwelijke gegevens dient steeds te gebeuren in versleutelde vorm. Dit geldt zowel voor informatie via analoge als digitale dragers. Wanneer de organisatie vertrouwelijke informatie toegestuurd krijgt, zelfs via een onveilige weg, dan moet deze volgens de classificatie van de betreffende gegevens opgeslagen worden. Het zelf versturen van vertrouwelijke gegevens zonder bijkomende veiligheidsmaatregelen is zonder meer verboden. Het lokaal synchroniseren van bv. agendagegevens is mogelijk voor zover er geen vertrouwelijke gegevens uitgewisseld worden.
- Er mogen geen documenten bij de printer achtergelaten worden.
- Verifiëren of de gegevens vrij zijn van virussen en andere kwaadaardige programmatuur die de bedrijfszekerheid van de systemen in het gedrang kunnen brengen:
    - het is verboden om de geïnstalleerde virusscanner uit te schakelen.
    - geconfronteerd met een virus, een verdachte e-mail of een verdacht document, moet onmiddellijk gestopt worden met werken op het ICT middel en moeten ze verwijderd worden; er moet steeds contact opgenomen worden met de ICT-dienst.
    - programmatuur en gegevens verkregen via een extern netwerk, via webtoepassingen (zoals o.a. webmail, webhosting, …), via externe ICT middelen (zoals o.a.

smartphones, tablets, laptops, …) of via draagbare media (zoals o.a. CD-ROM's, DVD's, USB sticks, ...) moeten gecontroleerd worden op virussen en andere kwaadaardige programmatuur.

- Melden van incidenten, eventuele lacunes in de beveiliging van het computersysteem of van methodes die de beveiliging van de gegevens in het gedrang brengen, bij de dienst ICT. Derden mogen hiervan niet op de hoogte worden gebracht. Het uitbuiten van deze zwakheden wordt beschouwd als (poging tot) inbraak.
- De diensthoofden en leidinggevenden kunnen een out-of-office boodschap op de mailbox van de gebruiker laten instellen indien de continuïteit van de dienstverlening dit vereist. De diensthoofden en leidinggevenden zullen nooit aan de ICT dienst vragen om het paswoord van de gebruiker aan te passen, tenzij bij overmacht.
- De organisatie beslist welke ICT-middelen er ondersteund worden en welke niet.
- Bij verlies of diefstal moet dit direct aan de ICT dienst gemeld worden. Indien er persoonsgegevens op staan wordt dit gemeld aan onze DPO die dit zal melden als datalek.
- Wanneer noodzakelijk (bv. bij diefstal of verlies) mag de organisatie alle of gedeeltelijke toegangen van de ICT-middelen (zoals bv. smartphones, tablets, laptops, …) die aangesloten zijn op het intern netwerk, blokkeren. De dienst ICT mag, bij beheerde toestellen of als het toestel bij de organisatie geregistreerd is, de data en applicaties op de ICT-middelen op afstand wissen en indien nodig de toestellen onbruikbaar maken. Bij externe ICT-middelen die geen eigendom zijn van de organisatie gebeurt dit in samenspraak met de eigenaar.
- Er mag geen data van het lokaal bestuur opgeslagen worden op een eigen smartphone, tablet, notebook, desktop pc, … .

1.3. Ongeoorloofd gebruik

De organisatie laat het gebruik van de ICT-middelen niet toe: (deze lijst is niet uitputtend)

- om informatie te raadplegen, verspreiden of op te slaan die:
  - het imago, de morele of economische belangen van de organisatie kan schaden.
  - beledigend, lasterlijk, aanstootgevend of discriminerend is.
  - schade kan toebrengen aan derden.
  - strijdig is met de openbare orde of goede zeden.
  - Beschermd zijn door auteursrechten en die bij wet beschermd zijn tegen schending
- om vertrouwelijke informatie door te geven.
- om vertrouwelijke informatie onbeschermd te bewaren zowel elektronisch als op papier noch een kopie te bewaren.
- om software te installeren of te gebruiken waarvoor de dienst ICT geen toestemming heeft verleend.
- het doorsturen ("forwarden") naar een eigen persoonlijk e-mailadres;
- om mee te werken aan "kettingbrieven" (e-mails die je ontvangt en vervolgens aan x-aantal personen moet doorsturen met het oog op b.v. het winnen van een prijs, …);
- internet te gebruiken voor illegale activiteiten, ongeacht de aard ervan.
- sites bezoeken waarvan de inhoud geen enkele informatieve waarde bevat en die louter zijn gecreëerd met doel te dienen tot ontspanning of vermaak;
- om systeeminformatie, systeemconfiguratie, toepassingsprogramma's of bestanden te wijzigen, te verwijderen of door te geven aan derden, indien men daarvoor uit hoofde van zijn functie niet toe is gerechtigd. Software kan enkel geïnstalleerd worden door de ICT dienst.

1.4. Toegelaten persoonlijk gebruik van ICT-middelen

De ICT-infrastructuur kan beperkt en occasioneel voor privédoeleinden gebruikt worden voor zover:

- dit gebeurt buiten de werkuren van de medewerker.
- het personeel dat nog of reeds aan het werk is, niet wordt gestoord.
- persoonlijke bestanden of gescande files niet opgeslagen worden op de ICT-infrastructuur van de organisatie.
- dit geen gevolg heeft voor de goede werking van het netwerk.
- er geen kosten verbonden zijn aan het gebruik van de middelen

De organisatie heeft het recht om, wanneer dit om bedrijfsredenen vereist wordt of wettelijk bepaald:

- 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.
- op ieder moment zonder voorafgaande waarschuwing de toegang tot bepaalde websites, apps, betaalnummers en (interne en externe) toegangen af te sluiten en (tijdelijk of permanent) te verbieden.

1.5. Uitdiensttreding personeelslid

Indien mogelijk wordt aangeraden om de kwestie van de mailbox ter regelen vóór het vertrek van de werknemer. Indien het voor de goede werking van de organisatie nodig blijkt te zijn om een deel van de inhoud van de mailbox te recupereren, moet dit gebeuren in het bijzijn van de werknemer en vóór het vertrek van de werknemer. Bij een geschil is de tussenkomst van een vertrouwenspersoon aanbevolen als het Lokaal Bestuur vreest dat de betrokken werknemer opzettelijk professionele gegevens zou lekken.
De mailbox van een werknemer die niet meer in dienst is, wordt zo snel mogelijk geblokkeerd. De organisatie voert hiervoor een automatisch bericht in dat iedere latere correspondent ervan verwittigt dat de werknemer niet langer meer in dienst is.
De mailbox wordt ten laatste twee weken na het vertrek van de betrokken werknemer afgesloten.
Het professionele e-mailadres van de vroegere werknemer mag in geen geval nog verder worden gebruikt door de werkgever. Dergelijke handelingen komen neer op naamvervalsing of -verduistering en zijn strafbaar.

1.6. Controle

De Algemeen Directeur, het diensthoofd P&O, de ICT-verantwoordelijke en alle leidinggevenden van de organisatie waken over de naleving van dit reglement.
De Algemeen Directeur of het diensthoofd P&O kan het gebruik van internet, e-mail en andere communicatiemiddelen permanent of tijdelijk laten controleren door de dienst ICT. Dit gebeurt desgevallend met eerbiediging van de regelgeving op de privacy.
Controle op het communicatiegebruik gebeurt enkel met het oog op:

- 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 veiligheid en/of de goede technische werking van het ICT-netwerksysteem, met inbegrip van de controle op de kosten die ermee gepaard gaan, alsook de fysieke bescherming van de installaties van het lokaal bestuur
- het te goeder trouw naleven van de regels rond gebruik van ICT-middelen zoals vermeld in het onderhavige beleid.

De Algemeen Directeur of het diensthoofd P&O zal via de dienst ICT in zijn controle niet verder gaan dan nodig is voor het verwezenlijken van deze doelstellingen. Men kiest de controlemethode die de geringst mogelijke inmenging in de persoonlijke levenssfeer van de medewerker tot gevolg heeft. De dienst ICT kan een algemene lijst van de elektronische onlinecommunicatie-gegevens bijhouden. De resultaten worden elektronisch geregistreerd en bijgehouden gedurende een periode van vier maanden. Nadien worden ze verwijderd, tenzij zij het voorwerp uitmaken van een onderzoek. Indien ernstige vermoedens ontstaan van misbruik of onregelmatigheden, dan kan de Algemeen Directeur de dienst ICT de opdracht geven de elektronische online communicatiegegevens te verwerken om ze aan een geïdentificeerde of identificeerbare persoon toe te schrijven. Gegevens of communicatie waarvan niet uitdrukkelijk is aangegeven dat het gaat om privé-informatie, kunnen op elk moment door de Algemeen Directeur worden ingekeken. Privécommunicaties kunnen bij ernstig vermoeden van misbruik of van niet-naleving van het beleid gecontroleerd worden op hun aantal, tijdstip en/of hun inhoud in het bijzijn van de betrokken gebruiker.

1.7. Sancties

Sancties kunnen worden opgelegd conform het arbeidsreglement.