BIJLAGE 5: ICT-REGLEMENT

Doelstellingen

De goede werking van de organisatie is sterk afhankelijk van de vlotte en doeltreffende werking van de Informatie en Communicatie Technologie (ICT) en de manier waarop medewerkers ermee omgaan. Daarom worden naast de afspraken die in de deontologische code en de gedragscode sociale media zijn opgenomen, ook afspraken gemaakt vanuit welke waarden en normen het personeel omgaat met de ter beschikking gestelde ICT-middelen en welk gedrag daaraan voldoet.

De code geldt voor alle medewerkers, mandatarissen en externen die toegang hebben tot de ICT-middelen.

Welke ICT-Middelen worden bedoeld?

De eigen medewerkers en bepaalde medewerkers van andere organisaties die bij de organisatie een opdracht uitvoeren een aantal informatie-, communicatie- en technologiemiddelen voor de uitoefening van hun taken.

De ICT-middelen kunnen opgesplitst worden in:

- ICT-systemen (hardware en software);
- Informatie op ICT-systemen.

Hardware en software zijn bijvoorbeeld:

- e-mail en internetfaciliteiten;
- computers, laptops, “thin-clients”,..;
- smartphone, tablet, vaste telefoon
- badgelezer
- printers;
- USB-sticks;
- opslagmedia (bijvoorbeeld een server),…

De informatie op de ICT-systemen behoort ook tot de ICT-middelen.

Hoe omgaan met ICT-middelen?

§1 Zorgvuldig beheer van ICT-middelen

Met de ICT-middelen die gebruikt worden tijdens het werk ga je om als een zorgvuldig en vooruitziend persoon. Gebruik van de ICT-middelen is enkel toegestaan op voorwaarde dat het de goede werking en de belangen van het bestuur niet schaadt. Elk gebruik dat indruist tegen de principes van deze richtlijnen of dat in strijd is met de instructies die door het bestuur worden gegeven is niet toegestaan.

Geef geen toegang aan derden (vreemd aan het bestuur) tot het netwerk van de organisatie en de bijhorende toepassingen of apparatuur, op welke wijze ook, tenzij een wet of regelgeving hiertoe verplicht. In dat laatste geval blijf je ertoe gehouden je voorafgaandelijk ervan te vergewissen dat deze persoon kennis heeft van de richtlijnen. Je vergewist je ervan dat deze persoon deze zal naleven.

Daarnaast ben je bereid verantwoording af te leggen over het gebruik van ICT-middelen.

De middelen dienen om het algemeen belang na te streven. Bijgevolg worden deze gebruikt met het oog op efficiëntie en effectiviteit.

Hier gelden volgende specifieke afspraken voor het omgaan met ICT-middelen :

- Het gebruik van de ICT-middelen is:
  - steeds in overeenstemming met de doelstellingen.
  - niet bestemd voor commerciële doeleinden.
  - niet voor discriminatie, pesten, stalking, spamming,…
- Gebruik de ICT-middelen op een wettelijke manier met respect voor het auteursrecht en de privacy.
- Neem contact op met de ICT dienst om nieuwe software te installeren. Zelf aanpassingen uitvoeren op de computer, software enz. is verboden. Het zichzelf toegang verschaffen of derden toegang verschaffen tot onze systemen en hardware is niet toegestaan zonder toestemming van de ICT dienst.
- Blijf beleefd en professioneel in je online communicatie, voer geen verhitte discussies en pas op met cynisme en sarcasme. Geschreven berichten komen soms anders over dan bedoeld.
- Bezoek geen sites die zich tegen de grondbeginselen van de democratie en de rechtstaat keren, die kwetsend of beledigend zijn, die in strijd zijn met de goede zeden of die een gevaar voor verslaving vormen of sites die aanzetten tot discriminatie wegens ras, etnische afkomst, godsdienst, enz..
- Verstuur geen kettingmails, virussen of valse virusmeldingen. Als u een virus of valse virusmelding ontvangt, waarschuw dan de ICT-dienst.
- Als u verdachte spamberichten of andere verdachte berichten in uw mailbox ontvangt Waarschuw dan de ICT- dienst.
- Spring voorzichtig om met je wachtwoorden.

De medewerker respecteert de regels m.b.t. de digitale identiteit:

- Hij verschaft zich enkel toegang tot de ICT-middelen met de hem of haar toegewezen identiteit;
- Hij is persoonlijk aansprakelijk voor alle handelingen die worden uitgevoerd onder diens identiteit, en geeft dit wachtwoord aan niemand door (ook niet aan een hiërarchisch overste of aan ICT);
- Bij een vermoeden dat zijn of haar wachtwoord door een ander gekend is, stelt hij dit onmiddellijk en uiterlijk binnen de 24 uur opnieuw in.
- Beveilig de informatie die u zelf door middel van ICT gebruikt en stuur nooit informatie door via internet zonder dat specifieke veiligheidsmaatregelen worden genomen;
- De informatie die je opslaat op het ter beschikking gestelde materiaal blijft eigendom van het bestuur en moet steeds toegankelijk zijn voor de behoeften van de dienst.

§2 Tijds- en plaats onafhankelijk werken.

Door de toename van het tijds- en plaats onafhankelijk werken en de moderne informaticamogelijkheden zijn de grenzen tussen privé en werk vaak minder duidelijk. Als je documenten en materiaal mee op verplaatsing neemt (bv. naar huis), tref je de nodige maatregelen om die informatie te beschermen, zowel thuis als onderweg. Respecteer de bestaande afspraken in je organisatie, zowel de algemene afspraken als de afspraken binnen je entiteit.

Het gebruik van alle ICT-apparatuur blijft beperkt tot zakelijke en professionele doeleinden.

Alle authentificatiemiddelen (paswoorden, e-id., tokens, bankkaarten, enz.) mogen nooit samen of in de buurt van een pc of laptop bewaard worden. Bij verlies of diefstal zal de verantwoordelijke van de dienst en de ICT-verantwoordelijke onmiddellijk verwittigd worden zodat de nodige maatregelen genomen kunnen worden.

Het bewaren van gevoelige gegevens op de lokale computer of op gegevensdragers moet zoveel mogelijk vermeden worden. Indien dit toch zou gebeuren moet dit steeds op een versleutelde en beveiligde manier gebeuren.

De toestellen zijn voor professioneel en individueel gebruik. Laat geen gezinsleden of derden met de apparatuur werken.

Het aansluiten van privé apparatuur of privé netwerken is niet toegelaten zonder uitdrukkelijke toestemming van de ICT-dienst.

§ 3 Behoorlijk e-mail- en internetgebruik.

De algemeen directeur bepaalt of een personeelslid voor zijn functie over internet en e-mail moet kunnen beschikken. Het gebruik ervan gebeurt onder het toezicht en de verantwoordelijkheid van de diensthoofden.

Elk internetgebruik met een duidelijke link naar het werkkader binnen de werkuren is toegestaan.

Beperkt privégebruik van het internet is toegestaan voor zover je de uitvoering van je taken en de productiviteit van jezelf en die van je collega-medewerkers niet in het gedrang brengt. Dit een gunst en geen recht. Het lokaal bestuur kan te allen tijde het privégebruik beperken, wanneer de richtlijnen niet worden nageleefd.

Het is echter niet toegestaan om bepaalde sites (zie §1 en rubriek 'controle') te bezoeken en bestanden voor privédoeleinden te downloaden.

Zonder limitatief te zijn, worden volgende activiteiten in ieder geval ten strengste verboden, zelfs in het kader van de uitvoering van de functie:

- Vertrouwelijke informatie over het bestuur, zijn opdrachten of zijn personeel verspreiden, behalve indien de functie dit op een redelijke manier eist;
- Gegevens verspreiden of downloaden die beschermd zijn door auteursrechten en die bij de wet beschermd zijn tegen schending;
- Elektronische berichten naar anderen doorsturen ('forward') wanneer er geen gerechtvaardigde professionele reden bestaat, bijvoorbeeld bij omstandigheden waarin afbreuk gedaan wordt aan de persoon die het originele bericht geschreven heeft;
- Berichten doorsturen of sites bezoeken waarvan de inhoud de waardigheid van de anderen in gevaar kan brengen, namelijk het doorsturen of bezoeken van racistische of revisionistische sites, of sites die discriminerend zijn op basis van geslacht, seksuele geaardheid, handicap, godsdienst of politieke overtuigingen van een persoon of een groep personen;
- Berichten, beelden of bijlagen doorsturen of op aanvraag ontvangen, die door het volume de goede werking van de ICT-infrastructuur kunnen beïnvloeden;
- Persoonlijke interne of externe berichten doorsturen die niets te maken hebben met de functie (teksten, mopjes, prentjes, video's,...), gezien de belangrijke risico's die deze kunnen

inhouden (lijnen blokkeren, virussen verspreiden, ...) wanneer ze doorgestuurd worden via internetsites die niet tot het gemeentelijke netwerk behoren;

- 'uitvoerbare' bestanden doorsturen en/of, in geval van ontvangst, openen; deze vormen immers een ernstige bedreiging voor de stabiliteit en de veiligheid van het netwerk;
- Erotische of pornografische sites bezoeken, zelfs als ze bij de wet toegestaan zijn;
- Interne of externe e-mailberichten en internet gebruiken voor een professionele activiteit die niets te maken heeft met de opdracht van de medewerker;
- Aan 'kettingbrieven' meewerken;
- Meer algemeen, zowel de interne als de externe elektronische briefwisseling of het internet gebruiken voor een illegale activiteit, van om het even welke aard.
- Het verzenden van provocerende e-mailberichten;
- Het gebruik van e-mailberichten om bepaalde situaties binnen het bestuur openlijk aan te klagen;
- Het verzenden van e-mailberichten 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 verband houden met spelen en weddenschappen, verdovende middelen of vormen van fraude;
- Elk gebruik van het e-mailsysteem in het kader van een onwettige activiteit, welke ook, of in strijd met wettelijke bepalingen. De gebruikers worden dienaangaande gewezen op de verplichtingen die voortvloeien uit de Wet van 28 november 2000 inzake computercriminaliteit, dat o.m. volgende feiten strafbaar stelt (art. 550 bis Strafwetboek):
- Kennisname van informaticagegevens van personeelsleden door gebruik van andermans paswoord;
- Kennisnemen van informaticagegevens van personeelsleden of derden door het zich toegang te verschaffen tot een netwerk, een server of een bestand zonder daartoe de toestemming te hebben ('hacken');
- Kennisname van door hacking verkregen gegevens;
- Het downloaden van software zonder toestemming van de systeembeheerder;
- Deelnemen aan chatrooms, newsgroups,... ongeacht het onderwerp waarover zij handelen, tenzij hiervoor schriftelijke toestemming gegeven is door de algemeen directeur;
- Het consulteren van games of goksites.

Bij twijfel aangaande de geoorloofdheid van een gebruik van e-mail, dient de medewerker zich te wenden tot de algemeen directeur.

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 algemeen vreemd zou zijn aan de activiteiten van het bestuur.

Het gebruik van onveilige online filesharing diensten die toelaten om veel en/of grote bestanden te delen en op te laden is niet toegestaan. De medewerker moet voorafgaandelijk nagaan bij ICT welke online filesharing diensten wel veilig en toegelaten zijn of welke tools de medewerker moet gebruiken om bestanden veilig uit te wisselen.

Wat **e-mail** betreft, is het gebruik van de officiële e-mailadressen van het bestuur **enkel voor professionele doeleinden** toegestaan, voor zover:

- de uitgewisselde informatie ondubbelzinnig gelinkt is aan je taken;
- in de e-mail geen vertrouwelijke informatie wordt meegedeeld waartoe je geen bevoegdheid hebt om deze mede te delen;
- de geldende stijlregels worden nageleefd.

Het feit dat het emailadres de persoonlijke naam bevat, betekent niet dat alle email een persoonlijk karakter krijgt. Vanuit het professioneel account mogen geen privémails verstuurd en ontvangen worden.

Bij het verzenden van een extern bericht voorzie je steeds een visuele handtekening.

Je handtekening moet minimaal een aantal vermeldingen bevatten conform de huisstijl, zoals naam, voornaam, functie, coördinaten en e-mailadres.

Bij een geplande afwezigheid moet je steeds je “out-of -office reply” vooraf inschakelen. Je voorziet daarbij een korte afwezigheidsboodschap waarin op een professionele manier de aanvang en het einde van je afwezigheidsperiode vermeld staat. Vermeld daarbij ook het e-mailadres en/of telefoonnummer van de collega(‘s) van de betrokken dienst die men kan contacteren tijdens jouw afwezigheid.

Mails die verstuurd en ontvangen worden via de professionele account van de medewerker worden beschouwd als eigendom van het bestuur. Bij een onvoorziene afwezigheid is je directe leidinggevende of elke andere door jou aangestelde vertrouwenspersoon ertoe gerechtigd om je mailbox te controleren op inkomende e-mails. Het doel hiervan is de lopende zaken en de continuïteit van de dienstverlening te kunnen garanderen. De medewerker wordt hier altijd vooraf rond geïnformeerd.

Deze toegang is evenwel beperkt tot:

- E-mails die verband lijken te houden met lopende dossiers;
- Je afwezigheidsperiode waarin je correspondenten niet op de hoogte zijn van je afwezigheid.

Wanneer opgemerkt wordt dat tijdens de afwezigheid van de medewerker de opslagcapaciteit van zijn/haar mailbox bereikt is, wordt dit gemeld aan de systeembeheerder die volmacht krijgt om grote junkmails van een paar megabytes te verwijderen zodat mailverkeer opnieuw mogelijk is.

Alle e-mailverkeer verloopt via de officiële adressen van het bestuur (voornaam.naam@heusden-zolder.be of dienst@heusden-zolder.be). E-mail kan enkel gebruikt worden als communicatiemiddel, bevestiging van een telefoongesprek, enz. en heeft op zich geen bindend karakter.

De diensten moeten zich organiseren zodat hun mailbox dagelijks wordt gecontroleerd en een ontvangstbewijs dient zo vlug mogelijk te worden toegestuurd als de vraag niet onmiddellijk kan beantwoord worden.

Naast de hierboven vermelde voorschriften, moeten de volgende punten in acht worden genomen:

- geen enkel vraag onbeantwoord laten;
- zich niet laten meeslepen in polemieken;
- steeds hoffelijk blijven, zelfs tegenover brutale berichten;
- geen opmerkingen maken over personen, enkel over onderwerpen;
- symbolen, letterwoorden of referenties gebruiken die begrijpelijk zijn voor de ontvanger (dit houdt in geen speciale lettertypes te gebruiken die misschien niet herkenbaar zijn voor de ontvanger)

- kort en bondig zijn, of de lengte van het bericht op de eerste lijn vermelden wanneer dit twee bladzijden overschrijdt;
- het mag niet de bedoeling zijn om alle problemen op te lossen via e-mailcommunicatie. Persoonlijk contact dient eveneens een belangrijk communicatiemiddel te blijven binnen de organisatie.

De door te geven informatie moet duidelijk en gecontroleerd zijn: deze informatie mag geen aanleiding geven tot verwarring of vergissingen.

Alle officiële verbintenissen worden gedagtekend en ondertekend door de burgemeester en de algemeen directeur.

Het e-mail systeem is ook niet bedoeld voor het archiveren van belangrijke informatie of het verzenden van persoonsgegevens. Het systematisch doorsturen van werkmail naar persoonlijke mail is ook niet toegestaan.

Als je e-mailgegevens wil bewaren, moet je die bewaren op de juiste locatie op de servers en/of afdrukken en aan het dossier toevoegen.

Als je definitief je functie verlaat, moet je alle informatie meedelen die de voortzetting van de dienst mogelijk maakt. Zorg ervoor dat de ICT-middelen die je mocht gebruiken, na jou nog normaal gebruikt kan worden.

In geval van uitdiensttreding word je bij je vertrek de mogelijkheid geboden je private elektronische communicatie te recupereren of te wissen. Wanneer een deel van de inhoud van de mailbox moet worden gerecupereerd om de goede werking van het bestuur te waarborgen, zal dit gebeuren voor je vertrek en in jouw aanwezigheid.

Telefoon- en gsm-gebruik

In principe wordt telefonie enkel gebruikt voor de uitvoering van de arbeidstaak. Zorg ervoor dat je bereikbaar bent tijdens je arbeidsuren.

Het toestel dient gebruikt te worden als een goede huisvader. Gebruik je gsm-toestel tijdens het besturen van een voertuig enkel indien je handenvrij via bluetooth kan bellen.

Voor het factureren van telefonie en mobiele data wordt verwezen naar het arbeidsreglement.

Bepaalde gegevens inzake telecommunicatie kunnen gecontroleerd worden. Onder bepaalde gegevens verstaan we: inventarisering van de opgeroepen nummers, alsook het type, het tijdstip van aanvang en de duur van de oproepen, evaluatie van gemaakte telefoonkosten, … Kennisname van de inhoud van telefoongesprekken is niet toegestaan.

Veiligheidsmaatregelen

§1. Enkel de ICT-dienst of aangestelde derden mogen ICT-middelen installeren, demonteren, verplaatsen of wijzigen.

Er mag geen ander materiaal gebruikt worden dan de ICT-middelen die door de ICT-dienst en door de erkende leveranciers ter beschikking werden gesteld.

Enkel de software die rechtmatig aangekocht wordt, mag gebruikt worden. Deze moet toegelaten zijn met het oog op het specifieke karakter van de opdrachten en goedgekeurd zijn door de ICT-dienst.

Aansluitingen op externe netwerken zoals het internet, die niet toegelaten zijn, of die geïnstalleerd noch geconfigureerd zijn door de ICT-dienst, zijn verboden. Het gebruik van aansluitingen op externe netwerken en de e-mail moet beperkt blijven tot verrichtingen die absoluut noodzakelijk zijn voor de goede werking van de diensten.

Elke computer/desktop is voorzien van antivirussoftware. Indien dienst ICT merkt dat de antivirussoftware uitgeschakeld is, kan de toegang tot het netwerk onmiddellijk ontzegt worden. Gezien het groot belang van het correct gebruik van antivirussoftware voor onze organisatie, wordt het gebruik ervan te allen tijde gelogd.

Je verstuurt geen kettingbrieven, virussen of valse virusmeldingen. Als je een virus of valse virusmelding ontvangt, waarschuw dan dienst ICT. Dienst ICT neemt dan de nodige stappen en verwittigt het personeel.

Je bent alert voor kwaadaardige software (virussen, Trojaanse paarden, spyware, …) en internetcriminaliteit (internetfraude, phishing, social engineering, …). Om te voorkomen dat je hiervan het slachtoffer wordt:

- Je verandert nooit de veiligheidsinstellingen op jouw computer (firewall, antivirus, …)
- Je denkt steeds na over de context van het bericht (klopt het dat ik dit bericht ontvang van deze organisatie?)
- Je opent geen verdachte e-mails of bijlagen.

De dienst ICT zal hierover, in overleg met de informatieveiligheidscel, periodiek sensibiliseren, bv. door het organiseren van phishingtests.

Indien de medewerker het toestel onbeheerd moet achterlaten (vergadering, middagpauze,...) moet de pc vergrendeld worden (door middel van “windows” + L) of moet de gebruiker afgemeld worden. Computers worden automatisch vergrendeld via schermbeveiliging na maximum 20 min.

Printers en scanners mogen enkel worden gebruikt voor professionele doeleinden. Het gebruik van de printer wordt gelogd, waarop controle mogelijk is. De toegang tot deze middelen kan verleend worden door individuele authenticatie. Indien dit geval is , dan is deze code strikt persoonlijk.

TIPS:

- Druk informatie alleen af als je ze echt op papier nodig hebt.
- Laat afgedrukte documenten nooit bij de printer liggen.

§ 2 Sla je bestanden steeds op in de mappenstructuur of in de daartoe bedoelde toepassing die we hiertoe voorzien. Bestanden worden NIET op de harde schijf (c-schijf) bewaard. Gegevens die op een lokale harde schijf van de eigen pc bewaard worden, worden immers niet mee opgenomen in de dagelijkse back-up en dus kunnen al deze gegevens verloren gaan als er iets met je pc zou gebeuren.

Het kopiëren of overnemen van gegevens via diskettes, cd-rom's, USB-sticks of elk ander technisch middel, of van enig ander mobiel informatiedrager dan die van het bestuur, moet beperkt blijven tot de bestanden die absoluut noodzakelijk zijn voor de goede werking van de diensten. Het overzetten van informatie of gegevens van het bestuur mag enkel op mobiele informatiedragers die ter beschikking worden gesteld door het bestuur. De mobiele informatiedragers zijn beveiligd met een paswoord.

De opgeslagen informatie en deze informatiedragers blijven eigendom van het bestuur en moet steeds toegankelijk zijn voor de behoeften van de diensten. Dit is eveneens het geval vóór de medewerker definitief zijn functie verlaat. Hij/zij moet dan alle informatie meedelen die de voortzetting van de dienst en een normaal later gebruik van het informaticamateriaal dat tot zijn beschikking is gesteld, mogelijk maken.

§ 3 Als het ICT-middel abnormaal functioneert, dien je de ICT-dienst onmiddellijk te verwittigen en mag je het materiaal niet meer gebruiken.

§ 4 Je maakt op geen enkele manier een connectie van persoonlijke ICT-middelen met het netwerk van het lokaal bestuur, tenzij je toestemming hebt van de ICT-dienst. Als je zonder toestemming gebruik maakt van eigen ICT-middelen, zal je niet ondersteund worden door de ICT-dienst. Bij schade en of verlies van data veroorzaakt door bedrog, een zware fout of een lichte fout die eerder gewoonlijk dan toevallig voorkomt ben je zelf aansprakelijk. Het bestuur kan in dat geval niet verantwoordelijk gesteld worden voor beschadiging of diefstal van een persoonlijk toestel.

§5 Indien er ernstige aanwijzingen zijn van fraude, misdrijf of andere zware inbreuken op de verplichtingen van de medewerker, kan de algemeen directeur beslissen om de bestanden op de server van het lokaal bestuur en de individuele mappen van de medewerker op diens laptop te laten controleren. Deze controle gebeurt steeds met inachtneming van de geldende privacywetgeving en volgens het proportionaliteitsbeginsel. De raadpleging verloopt in aanwezigheid van de informatieveiligheidsconsulent of een andere daartoe aangeduide onafhankelijke persoon, die toeziet op het respecteren van de rechten van de medewerker. In die gevallen moet de betrokkene niet vooraf worden gewaarschuwd.

§6 Als preventiemiddel kan de toegang tot bepaalde internetsite geblokkeerd worden. Dit kan het geval zijn wanneer hun inhoud onwettig, beledigend of onaangepast zou zijn, of vreemd zou zijn aan de activiteiten van het bestuur. Het bestuur verwacht immers van medewerkers dat ze internet als werkinstrument gebruiken. Ook kan het veelvuldig bezoeken van bepaalde sites het netwerk belasten.

Controle

De algemeen directeur heeft het recht om controles te laten uitvoeren op het gebruik van internet en e-mail. Daarbij wordt het recht op het privéleven van de medewerkers gerespecteerd.

De controle wordt getoetst aan:

- Het finaliteitsbeginsel: een controle is alleen mogelijk voor de hieronder beschreven doeleinden;
- Het transparantiebeginsel: er wordt open gecommuniceerd over de controles en de doelen en voorwaarden van de controles;
- Het proportionaliteitsbeginsel: de controle en het soort controle moeten in verhouding staan tot het doel van de controle.

Die drie beginselen hebben als doel het evenwicht te houden tussen:

- Het recht van het bestuur op controle van werkmiddelen;
- Het recht van de medewerker op zijn privéleven.

Om deze controles mogelijk te maken registreren we onder andere de volgende gegevens:

- e-mail: het tijdstip, de grootte en de e-mailadressen van afzender en bestemmeling. De gegevens worden gedurende 2 jaar bewaard;
- internet: het connectietijdstip, de pc die de connectie aanvraagt en het IP-adres van de externe server. De gegevens worden gedurende 1 jaar bewaard.

Controle is alleen mogelijk voor de volgende doeleinden:

- Ongeoorloofde feiten vaststellen en voorkomen. Hiermee bedoelen we lasterlijke feiten, die strijdig zijn met de goede zeden of die de waardigheid van een andere persoon kunnen schaden, zoals:
- het kraken van computers, waaronder het op illegale manier persoonsgegevens of vertrouwelijke medische bestanden inkijken;
- het raadplegen van sites die:
    - zich tegen de grondbeginselen van de democratie en de rechtstaat keren, zoals sites die verband houden met racisme, terrorisme of discriminatie;
    - anderen kunnen kwetsen of beledigen, zoals sites met racistische of seksistische onderwerpen, pornografisch materiaal of schokkende foto's;
    - een gevaar voor verslaving vormen zoals goksites en pornografische sites;
    - iemands privéleven aantasten.
- Bepaalde informatie beschermen. Er zijn uitzonderingen op de principiële openbaarheid van bestuur, omdat bepaalde informatie niet geschikt is om algemeen gedeeld te worden. Een controle is mogelijk als de belangen (opgesomd in het bestuursdecreet van 7 december 2018) worden geschaad;
- De veiligheid, de performante of de goede technische werking van de ICT-systemen van het bestuur verzekeren. Daar hoort de controle op de bijbehorende kosten en de fysieke bescherming van de ICT-omgevingen (installaties) bij;
- Het te goeder trouw naleven en nagaan van de ICT-richtlijnen;
- De continuïteit van de dienstverlening verzekeren bij overlijden, onvoorziene afwezigheid of vertrek van een medewerker;

- Het nazien van logbestanden op het respecteren van de privacy of controle op de toegang tot bestanden (bv. informatie in authentieke bronnen).

§ 1 Algemene controle

De algemeen directeur kan voor de doelen (1) tot en met (4) een algemene controle doen op basis van globale gegevens (die geanonimiseerd en op niveau van de organisatie, afdeling of dienst geaggregeerd zijn), zoals:

- een lijst met oproepnummers, gespreksduur en gesprekskosten;
- een lijst van de bezochte websites, de frequentie en het volume van de doorgezonden informatie, maar niet de identificatie van de betrokken medewerkers die de sites hebben bezocht;
- het aantal en het volume van de uitgaande e-mails (niet de binnenkomende berichten), maar niet de identificatie van de betrokken medewerkers die ze hebben verstuurd.

§ 2 Individuele controle

Een individuele controle is toegestaan voor de volgende doelen en onder de volgende voorwaarden:

- indien uit een algemene controle blijkt dat iemand uit de gecontroleerde groep de ICT-middelen niet heeft gebruikt volgens de richtlijnen. De individuele controle kan in die situatie alleen nadat de algemeen directeur:
    - de betrokkenen heeft ingelicht over het bestaan van een onregelmatigheid;
    - het personeel op de hoogte heeft gebracht dat de globale gegevens geïndividualiseerd zullen worden als opnieuw een dergelijke onregelmatigheid vastgesteld wordt bij de volgende algemene controle.
- indien uit een algemene controle blijkt dat iemand uit de gecontroleerde groep zich schuldig maakt aan:
    - ongeoorloofde feiten, laster of feiten die strijdig zijn met de goede zeden of die de waardigheid van een andere persoon kunnen schaden;
    - het openbaar maken van vertrouwelijke informatie;
    - feiten die de veiligheid, de performante of de goede technische werking van de ICT-systemen van het bestuur in het gedrang brengen.

In die gevallen moet de betrokkene niet vooraf worden gewaarschuwd.

Indien er ernstige aanwijzingen zijn van fraude, misdrijf of andere zware inbreuken op de verplichtingen van de medewerker, kan de algemeen directeur beslissen om de bestanden op de server van het lokaal bestuur en de individuele mappen van de medewerker op diens laptop te laten controleren. Deze controle gebeurt steeds met inachtneming van de geldende privacywetgeving en volgens het proportionaliteitsbeginsel. De raadpleging verloopt in aanwezigheid van de informatieveiligheidsconsulent of een andere daartoe aangeduide onafhankelijke persoon, die toeziet op het respecteren van de rechten van de medewerker. In die gevallen moet de betrokkene niet vooraf worden gewaarschuwd.

Indien een medewerker overleden is, onvoorzien afwezig is of de dienst heeft verlaten en niet kan worden bereikt. In dat geval kan de leidinggevende diens werk gerelateerde e-mailverkeer en informatie op de opslagmedia raadplegen. Het doel daarvan is de continuïteit van de dienstverlening te garanderen. De raadpleging gebeurt via de informatieveiligheidsconsulent. Die kan dan nagaan welke berichten en informatie werk gerelateerd zijn en dus mogen worden ingezien door de leidinggevende.

In het kader van een onderzoek bij feiten van geweld, pesterijen en ongewenst seksueel gedrag. Daarbij is de algemeen directeur bevoegd om de verzamelde globale gegevens te individualiseren.

Bewaren van persoonlijke gegevens

De persoonlijke gegevens die worden verzameld tijdens een algemene of individuele controle worden bewaard gedurende een periode van maximaal 1 jaar.

Je hebt het recht om je persoonlijke gegevens (die werden verzameld tijdens de controle) in te kijken en om het bestuur te verzoeken eventueel foute gegevens te wijzigen of te schrappen.

Sancties

De medewerker die bij toepassing van de individualiseringsprocedure verantwoordelijk wordt gesteld voor een onregelmatigheid bij het gebruik van de ICT-middelen, wordt uitgenodigd voor een gesprek vóór enige beslissing of evaluatie die hem individueel kan raken; deze procedure op tegenspraak zal de medewerker in staat stellen het gebruik van de hem ter beschikking gestelde ICT-middelen te rechtvaardigen.

Naar aanleiding van elke inbreuk op deze richtlijnen kan het bestuur - na verloop van voormelde procedure – de nodige maatregelen treffen.

In dit kader geldt artikel 13 en 14 van dit Arbeidsreglement.

heusden zolder

Team Personeel & HR
Heldenplein 1 | 3550 Heusden-Zolder | 011 80 80 80