**BIJLAGE 2**

**ICT-REGLEMENT**

## Art. 1. – 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 personeelsleden 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.

## Art. 2. – Toepassingsgebied

De code geldt voor alle medewerkers, mandatarissen en externen die toegang hebben tot de ICT-middelen van het lokaal bestuur Holsbeek alsook op het gesubsidieerd onderwijspersoneel.

## Art. 3. – Welke ICT-middelen worden bedoeld?

Lokaal bestuur Holsbeek biedt haar medewerkers en bepaalde medewerkers van andere organisaties die bij de organisatie een opdracht uitvoeren een aantal informatie-, communicatie- en technologiemiddelen aan 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”,…
* vaste en mobiele telefoons
* tablet
* badgelezer
* printers, MFT
* USB-sticks
* opslagmedia (bijvoorbeeld een server),…

De informatie op de ICT-systemen behoort ook tot de ICT-middelen (vb. e-mailberichten, tekstbestanden, foto’s of muziek).

## Art. 4. – Hoe omgaan met ICT-middelen?

### 4.1. 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.

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

* Je gebruikt de ICT-middelen:
* steeds in overeenstemming met de doelstellingen
* niet voor commerciële doeleinden
* niet voor discriminatie, pesten, stalking, spamming,…
* Je gebruikt de ICT-middelen op een wettelijke manier met respect voor het auteursrecht en de privacy
* Je neemt contact op met de ICT dienst om nieuwe software te installeren. Je voert zelf geen aanpassingen uit op de computer of aan de software enz. Jezelf toegang verschaffen of derden toegang verschaffen tot de systemen en hardware is niet toegestaan zonder toestemming van de ICT dienst.
* Je blijft beleefd en professioneel in je online communicatie, voert geen verhitte discussies en past op met cynisme en sarcasme. Geschreven berichten komen soms anders over dan bedoeld
* Je bezoekt 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
* Je verstuurt geen kettingmails, virussen of valse virusmeldingen. Als je een virusmelding, spam of ander verdacht bericht ontvangt, waarschuw je onmiddellijk de ICT-dienst
* Je springt voorzichtig om met je wachtwoorden. Je gebruikt bij voorkeur een digitale sleutelkluis zoals bv. KeePass
* Je respecteert de regels m.b.t. de digitale identiteit:
* Je verschaft je enkel toegang tot de ICT-middelen met de jou toegewezen identiteit
* Je bent persoonlijk aansprakelijk voor alle handelingen die worden uitgevoerd onder jouw identiteit, en geeft dit wachtwoord aan niemand door (ook niet aan een leidinggevende of aan ICT)
* Bij een vermoeden dat je wachtwoord door een ander gekend is, stel je dit onmiddellijk en uiterlijk binnen de 24 uur opnieuw in
* Je beveiligt de informatie die je zelf door middel van ICT gebruikt en stuurt 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

### 4.2. Telewerken/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. Je respecteert de bestaande afspraken van de organisatie, zowel de algemene afspraken als de afspraken binnen de eigen entiteit.

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

Authentificatiemiddelen (paswoorden, eID, tokens, bankkaarten, enz.) bewaar je nooit samen of in de buurt van een pc of laptop. Bij verlies of diefstal verwittig je de verantwoordelijke van de dienst en de ICT-verantwoordelijke onmiddellijk 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, doe je dit steeds op een versleutelde en beveiligde manier.

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.

### 4.3. Behoorlijk internetgebruik

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

Het gebruik van onveilige online filesharing diensten die toelaten om veel en/of grote bestanden te delen en op te laden is niet toegestaan. Je checkt vooraf bij ICT welke online filesharing diensten wel veilig en toegelaten zijn of welke tools je kan gebruiken om bestanden veilig uit te wisselen.

### 4.4. Behoorlijk e-mail gebruik

Het gebruik van de officiële e-mailadressen van het bestuur is enkel toegestaan voor professionele doeleinden en voor zover:

* de uitgewisselde informatie ondubbelzinnig gelinkt is aan jouw taken
* je in de e-mail geen vertrouwelijke informatie meedeelt waarvoor je als medewerker geen bevoegdheid hebt om deze mee te delen
* je de geldende stijlregels naleeft

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

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

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

Inkomende en uitgaande e-mails met een officieel karakter registreer je in het digitaal archiveringssysteem van het bestuur (DiAS). Het e-mail systeem (Outlook) is immers niet geschikt, noch bedoeld voor het archiveren van belangrijke informatie.

Alle e-mailverkeer verloopt via de officiële adressen van het bestuur. E-mail kan enkel gebruikt worden als communicatiemiddel, bevestiging van een telefoongesprek, enz. en heeft op zich geen bindend karakter.

Alle officiële verbintenissen worden gedagtekend en ondertekend door de bevoegde instanties (al naargelang het geval: burgemeester en algemeen directeur, voorzitter van de raad en algemeen directeur of voorzitter BCSD en algemeen directeur).

Verzend geen persoonsgegevens via e-mail. Het systematisch doorsturen van werkmail naar je persoonlijke mail is ook niet toegestaan.

Als je definitief je functie bij het bestuur neerlegt, deel je alle informatie mee die de voortzetting van de dienst mogelijk maakt. Je zorgt er tevens voor dat de door jou gebruikte ICT-middelen ook na je vertrek nog normaal gebruikt kunnen worden.

## Art. 5. – Veiligheidsmaatregelen

* 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.
* Je slaat bestanden steeds op op de servers die hiertoe voorzien zijn.
* Als het ICT-middel abnormaal functioneert, verwittig je de ICT-dienst onmiddellijk en mag je het materiaal niet meer gebruiken.
* Je maakt op geen enkele manier een connectie van persoonlijke ICT-middelen met het netwerk van het lokaal bestuur, tenzij je hiervoor toestemming heeft van de ICT-dienst.
* Als je zonder toestemming gebruik maakt van eigen ICT-middelen, word je niet ondersteund 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 als medewerker zelf aansprakelijk. Het bestuur kan in dat geval niet verantwoordelijk gesteld worden voor beschadiging of diefstal van een persoonlijk toestel.
* Als preventiemiddel kan je toegang tot bepaalde internetsites geblokkeerd worden. Dit kan het geval zijn wanneer de inhoud ervan 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.

## Art. 6. – Controle

### 6.1. Internet en email

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 het nastreven van gerechtvaardigde doelen
* 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 registreert het bestuur o.a. volgende gegevens:

* e-mail: het tijdstip, de grootte en de e-mailadressen van afzender en bestemmeling. De gegevens kunnen tot 1 jaar bewaard worden
* internet: het connectietijdstip, de pc die de connectie aanvraagt en het IP-adres van de externe server. De gegevens worden gedurende 90 dagen bewaard

Controle is alleen mogelijk met de volgende bedoelingen:

* 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 van de ICT-richtlijnen
* De continuïteit van de dienstverlening verzekeren bij overlijden, onvoorziene afwezigheid of vertrek van een personeelslid
* Privacy loggings of controle op de toegang tot bestanden (bv. informatie in authentieke bronnen)

### 6.2. Algemene controle

De algemeen directeur kan voor de voorgaande doelen 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

### 6.3. 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 een personeelslid 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.

## Art. 7. – 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.

## Art. 8. – Sancties

### 8.1. Algemeen

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.

Voor de statutaire medewerkers is dit de tuchtprocedure. Voor de contractuele medewerkers geldt art. 30 van dit arbeidsreglement.

### 8.2. Kruispuntbank en Rijksregister

#### 8.2.1. Consultatie van vertrouwelijke gegevens

* Medewerkers die gebruik maken van de KSZ toepassing of het Rijksregister mogen enkel de persoonsgegevens inzamelen die ze nodig hebben voor de goede uitoefening van hun functie. Elke medewerker is verantwoordelijk voor de raadplegingen of opzoekingen op de KSZ of het Rijksregister die onder zijn login gebeuren
* Enkel gemachtigde medewerkers, mogen gegevens op de KSZ of het Rijksregister consulteren. Het is stagiairs, jobstudenten, externe medewerkers of andere niet- gemachtigde personeelsleden niet toegestaan informatie op te vragen op de kruispuntbank of het Rijksregister tenzij zij bij hun acties vergezeld worden door een gemachtigd medewerker. Het is gemachtigde medewerkers niet toegestaan om niet- gemachtigde personen opzoekingen op de KSZ of het Rijksregister te laten uitvoeren
* De gemachtigde medewerkers zijn ertoe gehouden maatregelen te treffen om het vertrouwelijk karakter van de opgevraagde gegevens te verzekeren en om ervoor te zorgen dat ze uitsluitend worden aangewend voor professionele doeleinden en voor het vervullen van hun wettelijke verplichtingen
* Iedere opvraging via het netwerk van de KSZ of het Rijksregister wordt gelogd en bijgevolg kan er steeds gecontroleerd worden welke medewerker binnen het lokaal bestuur deze opvraging heeft verricht
* Met de elektronische identiteitskaart kan iedere burger opvragen wie er zijn gegevens heeft geconsulteerd op de KSZ of het rijksregister. Gemachtigde medewerkers moeten dus steeds de gegrondheid van hun opzoeking kunnen verantwoorden

#### 8.2.2. Mededeling van vertrouwelijke gegevens

* Elke persoon die betrokken is bij de inzameling, de verwerking of de uitwisseling van persoonsgegevens in het kader van de sociale zekerheid of het Rijksregister is gebonden door het beroepsgeheim
* Als je een vraag krijgt omtrent persoonsgegevens afkomstig van de KSZ of het Rijksregister dan geef je deze niet meteen vrij. Controleer steeds even of de aanvrager wel degelijk recht heeft op deze informatie. Nog beter is het om enkel te antwoorden als de vraag officieel en schriftelijk aan het lokaal bestuur is gericht

#### 8.2.3. Schending

Volgende gedragingen of handeling met betrekking tot de Kruispuntbank en het Rijksregister zijn verboden:

* Het onrechtmatig gebruik van de kruispuntbank of het Rijksregister
* Zich toegang verschaffen tot de kruispuntbank of het Rijksregister teneinde schade te berokkenen aan het systeem, door het invoeren, beschadigen, uitwissen of wijzigen van gegevens of door het belemmeren of aantasten van de gegevensverwerking

#### 8.2.4. Strafbepalingen

* Kruispuntbank: wordt geregeld in afdeling 2: Art. 60 tot 71 van Kruispuntbankwet (inbreuken en strafbepalingen)
* Rijksregister: wordt geregeld in artikel 13 van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen