ICT-POLICY

Bepalingen betreffende de ICT-middelen

Inhoudstafel

HOOFDSTUK I. ONDERWERP EN SCOPE.

Inleiding

Deze policy heeft als doel:

- het personeel te informeren over het gebruik van de ter beschikking gestelde ICT-middelen, en hen aan te sporen hier ten volle gebruik van te maken;
- de integriteit van het informaticasysteem van de Stad te garanderen;
- de gegevens te beveiligen die onder de verantwoordelijkheid van de Stad vallen of betrekking hebben tot het privéleven van de personeelsleden of van burgers, en hun privacy te beschermen, in overeenstemming met het recht op bescherming van de persoonlijke levenssfeer;
- de bescherming van de online reputatie van de stad tegen misbruik door een personeelslid op openbare websites;
- de omkadering van de controle op het gebruik van ICT-middelen door personeelsleden.

Personeelsleden hebben een professioneel e-mailadres waar ze toegang hebben tot het internet, telefonie en elektronische communicatie, vanop hun vaste werkplek of eventueel mobiel. Dit document vertegenwoordigt het standpunt van de Stad betreffende het gebruik van het internet en ICT-middelen van haar personeelsleden alsook het monitoren van dit gebruik met respect voor de privacy. Overtreding van onderhavige richtlijnen kunnen aanleiding geven tot disciplinaire sancties.

Artikel 1. Begrippen

De onderstaande begrippen welke meermaals gebruikt worden in deze policy zijn als volgt gedefinieerd:

Het personeelslid	Ieder die werknemer is van de Stad, welk juridisch verband er ook met de werkgever is (statutair of personeelslid met een arbeidsovereenkomst, kabinetslid, stagiaire, aan de Stad gedetacheerde…). Niet inbegrepen is het onderwijzend personeel van het openbaar Onderwijs van de Stad.
De werkgever	De Stad en haar vertegenwoordigers aan wie het personeelslid verbonden is via een arbeidsovereenkomst of een statuut.
De policy	Het onderhavige document en al haar richtlijnen.
ICT-middelen	Een ruim begrip dat slaat op al wat het personeelslid gebruikt om verbinding te maken met het Internet of het netwerk, of om te communiceren, zij het materieel of digitaal, elektronisch of telefonisch, en in het bijzonder desktop computers, laptops, printers, vaste telefoons en mobile apparaten (tablets, smartphones, PDA's, …).
Het gegeven	Al wat opgeslagen en geklasseerd kan worden, op papier of digitaal, in letters en cijfers of met beeld of geluid.
Persoons-gegevens	"Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (...); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon" AVG artikel 4

Gegevens onderworpen aan de rechten van anderen	Gegevens onderworpen aan de rechten van anderen zijn gegevens die afhankelijk van de situatie enkel voor intern gebruik bedoeld zijn, enkel benaderd kunnen worden door een aantal gemachtigden, of die beschermd zijn door de wet.
AVG **Privacywet**	(EU) Verordening 2016/679 - Bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG **(algemene verordening gegevensbescherming)** De Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens
Het bestand	Verzameling geordende (computer) gegevens, bv. een tekstverwerkingsdocument, folders, afbeeldingen, …
openbare websites	Elke vorm van publieke communicatie op het internet. Enkele voorbeelden (let op, deze lijst is niet exhaustief): sites en apps van sociale netwerken (Facebook, Snapchat, LinkedIn, …), websites voor het delen van video's en foto's (Youtube, Instagram, …), blogs, forums of discussiegroepen (Reddit, Google Groups, …) , chatrooms, websites voor korte berichten (Twitter, …), websites voor gezamenlijk publiceren (Wikipedia, …), …
Functionaris voor gegevens-bescherming **(DPO)**	De onafhankelijke persoon die adviseert over en helpt bij de uitvoering van privacyregelingen, waaronder gegevensbescherming. "1. De functionaris voor gegevensbescherming vervult ten minste de volgende taken: a) de verwerkingsverantwoordelijke of de verwerker en de werknemers die verwerken, informeren en adviseren over hun verplichtingen uit hoofde van deze verordening en andere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen; b) toezien op naleving van deze verordening, van andere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen en van het beleid van de verwerkingsverantwoordelijke of de verwerker met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits; c) desgevraagd advies verstrekken met betrekking tot de gegevensbeschermingseffect-beoordeling en toezien op de uitvoering (...); d) met de toezichthoudende autoriteit samenwerken; e) optreden als contactpunt voor de toezichthoudende autoriteit inzake met verwerking verband houdende aangelegenheden, met inbegrip van de in artikel 36 (van de AVG) bedoelde voorafgaande raadpleging, en, waar passend, overleg plegen over enige andere aangelegenheid 2. De functionaris voor gegevensbescherming houdt bij de uitvoering van zijn taken naar behoren rekening met het aan verwerkingen verbonden risico, en met de aard, de omvang, de context en de verwerkingsdoeleinden" AVG artikel 39 Beschikbaar via privacy@brucity.be.

Chief Information Security Officer (CISO)	De persoon die strategieën voor de beveiliging van informatiesystemen opstelt en de beveiliging van dit systeem beoordeelt teneinde het te verbeteren. Bereikbaar via security@brucity.be
ICT-dienstverlener	Diegene die ICT-middelen ter beschikking stelt of uitbaat in een contractuele relatie met de Stad.

HOOFDSTUK II. BESCHIKBAAR STELLEN VAN ICT-MIDDELEN

Artikel 2.

Aan elk personeelslid van de Stad worden, naarmate hun functie, een aantal standaard ICT-middelen ter beschikking gesteld, met privégebruik als voordeel alle aard. Deze middelen blijven eigendom van de werkgever. Het personeelslid is verplicht goede zorg voor deze middelen te dragen.

Specifiek voor wat betreft de ter beschikkingstelling van mobiele telefoons, dient de werknemer ook het “beleid van de Stad Brussel inzake mobiele telefoons” te raadplegen, dat beschikbaar is op het intranet en dat een aanvulling vormt op deze ICT-policy.

Het personeelslid geeft in het geval van aflopen of stopzetten van zijn of haar tewerkstelling deze middelen, alsook al het bijhorende materiaal (tassen, etc.), terug aan zijn of haar (adjunct)informaticacorrespondent of indien deze afwezig zijn aan het centraal secretariaat, en dit ten laatste op de laatst gepresteerde dag.

In geval van diefstal van materiaal is het personeelslid verplicht dit aan te geven aan de politie en het proces-verbaal te bezorgen aan de servicedesk van i-City en de DPO zo snel mogelijk op de hoogte te brengen op het volgende adres: dpo@brucity.be

Artikel 3.

Een aantal ICT-middelen wordt gemeenschappelijk aan een deel of het geheel van het personeel ter beschikking gesteld. Ook hiervoor is het personeelslid verplicht zorg te dragen als een voorzichtig en redelijk persoon en met respect voor voorliggende ICT-policy.

Artikel 4.

De werkgever weerhoudt zich het recht om op elk moment en zonder waarschuwing toegang tot bepaalde websites of bestanden te ontzeggen, voor de veiligheid van het informaticasysteem in het algemeen, of om een van de verboden activiteiten, zoals opgenomen in deze ICT policy, te verhinderen.

Artikel 5.

Einde van het ter beschikking stellen: Alle door de werkgever aan zijn personeelsleden ter beschikking gestelde ICT-middelen blijven eigendom van de Stad. Alle in mappen, bestanden en/of e-mails verzonden, ontvangen en/of opgeslagen gegevens zijn en blijven eigendom van de stad, tenzij zij duidelijk als persoonlijk zijn aangemerkt (zie het onderstaand punt over privégebruik).

Na het vertrek van het personeelslid behoudt de Stad zich het recht voor om toegang te krijgen tot de professionele gegevens van het personeelslid, alsmede tot zijn/haar professionele e-mails, voor zover deze toegang noodzakelijk is voor de:

(1) continuïteit van een dienst of een functie, voor zover de onderbreking van die dienst

of functie onevenredige schade zou toebrengen aan de stad of aan derden,

(2) voor de oplossing van een doorslaggevend probleem, zoals de veiligheid van het informatiesysteem of de veiligheid van een derde partij.

De toegang is onderworpen aan het gemotiveerd advies van de DPO en het akkoord van de gemeentesecretaris. Deze toegang heeft alleen betrekking op gegevens die nodig zijn voor de continuïteit van de dienst of de functie en niet op gegevens of e-mails die overeenkomstig artikel 11 als persoonlijk zijn aangemerkt. Deze toegang kan enkel plaatsvinden binnen een periode van maximaal 3 maanden na het einde van de samenwerking. Na deze periode worden de gegevens en e-mails gewist.

In ieder geval, wordt de continuïteit van de dienst of functie geacht te zijn bereikt als het personeelslid vóór zijn/haar vertrek al de gegevens en e-mails die nuttig zijn voor de continuïteit van de dienst of functie heeft doorgegeven.

Dit artikel is niet in strijd met overleg dat binnen een wettelijk kader kan plaatsvinden, bijvoorbeeld in het geval van een gerechtelijke procedure.

HOOFDSTUK III. GEBRUIK VAN ICT-MIDDELEN OP DE WERKPLEK.

Artikel 6.

Alle onderstaande richtlijnen betreffende het gebruik, zijn van toepassing op al deze middelen, alsook op eigen ICT-middelen wanneer het personeelslid ervan gebruik maakt in het kader van zijn of haar werk en tijdens de werkuren (privé computer via VPN, eigen smartphone, …).

Het personeelslid dat vanop afstand werkt is aan dezelfde richtlijnen onderworpen als wanneer hij of zij zich op de normale werkplaats bevindt.

Het gebruik van ICT-middelen in het kader van het werk omvat het gebruik tijdens de werkuren, het gebruik op elk ogenblik van de door de stad ter beschikking gestelde professionele toepassingen en het gebruik van het internetnetwerk van de stad.

Sectie 1 - PROFESSIONEEL GEBRUIK.

Artikel 7.

Voor de richtlijnen betreffende een professioneel gebruik van ICT-middelen kan de directie strengere vereisten opleggen; Er wordt verwacht van de personeelsleden dat ze zich waar mogelijk houden aan de volgende goede praktijken:

Correspondentie	a) een officieel e-mailadres (onder bv. het domein brucity.be) gebruiken voor elke correspondentie, intern of met buitenstaanders in het kader van zijn of haar functie; b) regelmatig zijn of haar inkomende post bekijken, tijdig te antwoorden of eventueel te laten weten wanneer hij of zij pas gevolg zal kunnen geven aan het bericht; c) het aantal geadresseerden in e-mails beperken tot het absoluut noodzakelijke; d) een bericht louter als ‘dringend’ taggen indien dit echt nodig is;

	e) bij het foutief versturen van een e-mail proberen deze e-mail te herroepen, of deze foutief geadresseerde in te lichten van zijn of haar vergissing; f) bij de ontvangst van een herroeping van een e-mail deze niet te openen en onmiddellijk te verwijderen;
Handtekening en lettertype	g) de gestandaardiseerde e-mailhandtekening en het gestandaardiseerde lettertype gebruiken - deze worden vastgelegd door de cel Communicatie en zijn te raadplegen in het grafisch charter;
Out of office	h) bij afwezigheid van meer dan één dag een out-of-office bericht op te stellen - in dit bericht wordt de periode van afwezigheid vermeld alsook de perso(o)n(en) of dienst die in dringende gevallen gecontacteerd kunnen worden;
Bijlagen van e-mails	i) vermijden volumineuze bestanden in bijlage aan e-mails toe te voegen; j) naar een gedeelde map verwijzen i.p.v. bestanden aan e-mails toe te voegen;
Printen	k) afdrukken van e-mails en documenten zo veel mogelijk vermijden en de voorkeur te geven aan het projecteren en digitaal doorsturen ervan; l) documenten met vertrouwelijke of persoonsgegevens alleen afdrukken wanneer dit absoluut noodzakelijk of wettelijk vereist is.
Ruimte maken in je mailbox	m) de aanbevelingen die de Stad doet op gebied van ruimte maken in je mailbox te respecteren en in elk geval: • regelmatig zijn of haar mailbox op te kuisen en enkel berichten te bewaren die nog kunnen dienen ; • zijn of haar mailbox te archiveren alvorens belangrijke berichten en bestanden te verwijderen; belangrijke berichten en bestanden te bewaren buiten de mailbox. De mailbox dient niet als opslagruimte;
Kalender	n) de Outlookkalender volledig in te vullen met de momenten waarop hij of zij niet beschikbaar is,
Duurzaamheid	o) zijn of haar toestellen (schermen, pc's, …) uit te schakelen bij het verlaten van de werkpost, alsook de gedeelde toestellen (printers, elektronische borden, …) indien hij of zij als laatste de werkplaats verlaat.

Artikel 8.

Een disclaimer wordt automatisch toegevoegd aan verzending naar domeinen die niet rechtstreeks aan de Stad Brussel of haar ICT-dienstverlener verbonden zijn. Het personeelslid is verplicht deze intact te houden.

Artikel 9.

Het sturen van collectieve berichten aan al de leden van meerdere departementen of aan het geheel van het personeel van de Stad maakt het voorwerp uit van een bijzondere procedure:

Aanvraag	a) De aanvragen voor verzending moeten gericht worden aan het e-mailadres van de dienst Interne Communicatie van het Departement HR om na te gaan of, in functie van wat hier volgt, niets de verspreiding van dit bericht in de weg staat. Verder moet ook de verspreiding aan personeelsleden die niet gemakkelijk hun e-mailadres consulteren verzekerd worden, onder de verantwoordelijkheid van hun leidinggevende. b) De teksten die voorgelegd worden zullen voldoende goedgekeurd zijn door het betrokken departement/kabinet. De gegevens van de verantwoordelijke uitgever (dienst of persoon) zullen vermeld zijn, met inbegrip van het e-mailadres. c) Voor de berichten van categorie 2 tot 4 moeten de teksten ruim op voorhand bezorgd worden om de dienst Interne Communicatie de gelegenheid te geven de paginaopmaak en de verzending te verzorgen. Een minimale termijn van twee dagen is vereist.
Categorieën	d) De berichten zullen ingedeeld worden volgens hun belangrijkheid (voorbeelden): CAT1: Organisatie van het werk = stroomonderbrekingen, technische interventies en onderhoudswerken aan het netwerk, de telefonie, enz., wijzigingen van het reglement; CAT 2: Werkaanbiedingen = oproepen tot mobiliteit, aanwerving, Selor, vormingen, ...; CAT 3: Gratis uitnodiging of voordeel voor het Stadspersoneel; CAT 4: Evenement = zuivere publiciteit (als er geen voordeel is voor de personeelsleden).
Inhoud	e) De aanvrager zal de tekst beperken tot maximaal 250 woorden per taal. Links naar intranet en internet zijn toegelaten. f) In de berichten zullen de namen van de schepenen vervangen worden door “Het College”.
Tweetaligheid	g) Volledige tweetaligheid (Frans/Nederlands) is van toepassing, zowel in de tekst van het bericht als in de eventuele bijlagen (.pdf, beeld met tekst, enz.). Rekening houdend met de wetgeving betreffende het gebruik van de talen zal de aanvrager, indien er verwijzingen zijn naar andere websites (Stad of andere), ook de links geven in de beide talen.
Bijlagen	h) De eventuele bijlagen dienen in veelvoorkomende formaten geleverd te worden, bv. .jpg (tekening of foto), .doc (Word), .xls (Excel), .pdf (Acrobat) en zeker niet uit gescande documenten te bestaan.
Verspreiding	i) In geval van verschillende, gelijktijdige aanvragen zal de dienst Interne Communicatie van het departement HR kunnen beslissen over de volgorde van verzending, om erover te waken de frequentie van één bericht per dag niet proberen te overschrijden. j) Indien niet anders aangeduid zal de verspreiding gebeuren aan het geheel van de personeelsleden van de Stad. Op aanvraag kan de verzending ook meer gericht gebeuren, zolang het groepen of lijsten betreft die voorzien zijn in Outlook; bv. “College”, “Departementen”, enz.

Opschorting, aanpassing of weigering.	k) De mails die te laat ontvangen worden of die niet stroken met de bepalingen van dit reglement mogen door de Dienst Interne Communicatie van het departement HR later verstuurd worden. Deze Dienst kan ook vragen de mail aan te passen aan het reglement en, indien dit niet gebeurt, de verzending van de mail weigeren.
Geen afwijkingen	l) Het is verboden dit soort berichten op een andere manier te versturen.

Sectie 2 - PRIVÉGEBRUIK.

Artikel 10.

Overeenkomstig de huidige federale wetgeving is privégebruik buiten de werkdag inherent aan het bezit van een laptop en vormt het een voordeel alle aard.

In elk geval is het privégebruik van ICT-middelen voor werkdoeleinden niet toegestaan indien het :

a) frequent en van lange duur is;
b) een impact heeft op de plichten van het personeelslid of zijn of haar medewerkers;
c) een impact heeft op de werking van de Stad;
d) extra kosten voor de Stad tot gevolg heeft;
e) in strijd is met andere onderdelen van deze policy;
f) in strijd is met de privacywet.

Ter informatie, enkele voorbeelden van toegestaan persoonlijk gebruik:	een eenvoudige online banktransactie uitvoeren; een korte persoonlijke e-mail opstellen; een kort telefoongesprek houden; uitzonderlijk enkele pagina's afdrukken voor persoonlijk gebruik.
Ter informatie, enkele voorbeelden van niet toegestaan persoonlijk gebruik	op uitgebreide wijze elektronische documenten voor persoonlijke doeleinden invullen; een boek kopiëren of uitprinten; telefoneren naar het buitenland; opzoekingen in beroepsapplicaties voor persoonlijke doeleinden. kettingmails verspreiden, spelletjes spelen, tijd in online chatrooms doorbrengen en dergelijke meer ; langdurig muziek en/of video streamen die niet in het kader van het werk te plaatsen vallen; grote bestanden downloaden; persoonlijke aangelegenheden met winstoogmerk aangaan, of reclame maken voor belangen vreemd aan die van de Stad.

Artikel 11.

Privégebruik van het professioneel e-mail adres kan indien het personeelslid de uitgaande e-mails als persoonlijk kenmerkt en het volgende toevoegt aan het bericht: "de inhoud van dit bericht is persoonlijk en kan in geen enkel geval leiden tot de aansprakelijkheid van de Stad Brussel".

E-mails met een persoonlijk karakter moeten tevens bewaard worden in een Outlookmap met de titel “privé”, indien men wil dat de Stad deze e-mails niet kan consulteren.

Elke e-mail die niet wordt aangeduid als “persoonlijk”, wordt beschouwd als professionele e-mail, hetgeen toegang tot deze e-mail kan impliceren in geval dat men de mail moet recupereren, met name aan het einde van de samenwerking om de continuïteit van de functie te waarborgen (zie artikel 5).

Artikel 12.

Privégegevens mogen enkel worden opgeslagen in een folder genaamd “privé” op de lokale schijf (harde schijf van de pc), indien men wil dat de Stad deze gegevens niet kan consulteren. Deze folder mag geen professionele gegevens bevatten. In het geval van stopzetten of aflopen van het contract en/of teruggave van ICT-middelen is het personeelslid verplicht deze gegevens zelf te recupereren voor het einde van de samenwerking, waarna ze automatisch worden verwijderd.

Sectie 3 - NIET TOEGESTAAN GEBRUIK OP HET NETWERK VAN DE STAD

Artikel 13.

Geen enkel personeelslid mag websites bezoeken, berichten versturen of beantwoorden met waarvan de inhoud :

- van erotische of pornografische aard is
- getuigt van racisme of vreemdelingenhaat ;
- discriminerend is op basis van geslacht, seksuele geaardheid, handicap, geloof, filosofische of politieke overtuigingen;
- revisionistisch is;
- pestgedrag of ongewenste intimiteiten bevat of bevorderend is;
- respectloos is ten opzichte van anderen;
- of dergelijke meer dat in strijd is met de goede zeden of de waardigheid van anderen aantast.

HOOFDSTUK IV. ONGEOORLOOFD GEBRUIK VAN ICT-MIDDELEN, OOK BUITEN DE WERKCONTECT

Sectie 1 - GEBRUIK TEN NADELE VAN DE STAD

Artikel 14.

Het is voor het personeelslid verboden, ook buiten de werkuren:

Onwettig gebruik	a) om elke vorm van fraude, piraterij, hacken, online gokken, drugsverkoop, inbreuk op auteursrechten … of andere onwettige activiteiten aan te gaan;
Verspreiding van vertrouwelijke gegevens en persoonsgegevens	b) om gegevens onderworpen aan de rechten van anderen die betrekking hebben op de Stad, haar instellingen, personeelsleden, diensten, zakenpartners, klanten of andere belanghebbenden te verspreiden behalve in het kader van zijn of haar plichten; c) om gegevens onderworpen aan de rechten van anderen of persoonsgegevens op te zoeken in toepassingen van de Stad voor persoonlijke doeleinden;

	d) om gegevens onderworpen aan de rechten van anderen of persoonsgegevens op ongeoorloofde wijze te raadplegen of communiceren; e) om gegevens onderworpen aan de rechten van anderen of persoonsgegevens te delen met derden, zelfs in privécommunicatie;
Laster	f) om de Stad, haar instellingen, diensten, personeelsleden, zakenpartners, klanten of andere belanghebbenden belasteren;
Verspreiding van eigen mening	g) de officiële handtekening te gebruiken in privécorrespondentie; h) om eigen meningen te laten voordoen als een officieel standpunt van de Stad, of ongeoorloofd in haar naam te spreken.

Sectie 2 - BETREFFENDE DE OPENBARE WEBSITES.

Artikel 15.

Specifieke regels betreffende het professioneel gebruik, d.w.z. de medewerkers die gemachtigd zijn om zich in naam van de Stad of uit te drukken of de Stad op openbare websites te vertegenwoordigen, worden beheerd door de diensten Communicatie en maken geen onderdeel uit van deze policy.

In elk geval is het voor elk personeelslid die niet over dergelijke machtiging beschikt verboden om op openbare websites actief te zijn terwijl hij of zij zich voordoet als de Stad of handelend in naam van de Stad. Het is het hem of haar wel toegestaan om in zijn of haar account de Stad als werkgever op te geven, mits vermelding dat het gaat om een persoonlijk account. Het is ook toegestaan om berichten gepubliceerd door de officiële accounts van de Stad te delen.

Artikel 16.

Alle bepalingen uit deze policy betreffende het gebruik van ICT-middelen zijn ook van toepassing op het gebruik van openbare websites (sociale media, forums,…) op de werkplek of bij verplaatsing in het kader van zijn of haar werk of bij telewerken.

In ieder geval is het de medewerker te allen tijde op openbare websites, ook op persoonlijke ICT-middelen en buiten de werkuren, verboden om

Inhoud strookt niet met de deontologie	a) openbaar inhoud te publiceren of in interactie te gaan over inhoud die : i. van laakbare pornografische aard is, zoals kinderporno of beelden van seksueel geweld; ii. getuigt van racisme of vreemdelingenhaat ; iii. discriminerend is op basis van geslacht, seksuele geaardheid, handicap, geloof, filosofische of politieke overtuigingen; iv. revisionistisch is; v. pestgedrag of ongewenste intimiteiten bevat of bevorderend is; vi. of dergelijke meer dat in strijd is met de goede zeden of de waardigheid van anderen aantast
Gegevens onderworpen aan de rechten van anderen en/of persoonsgegevens	b) Gegevens onderworpen aan de rechten van anderen of persoonsgegevens die betrekking hebben op de Stad, haar instellingen, personeelsleden, diensten, zakenpartners, klanten of andere belanghebbenden te verspreiden;
Laster	c) de Stad en haar instellingen, personeelsleden, diensten, zakenpartners en andere belanghebbenden te belasteren;

Onjuiste gegevens	d) leugenachtige, misleidende of verwarring zaaiende uitspraken te doen betreffende de Stad en haar instellingen, personeelsleden, diensten, zakenpartners en andere belanghebbenden; e) zich voor iemand anders uit te geven die verbonden is aan de Stad; f) foutieve informatie inzake zijn of haar professionele ervaring of verantwoordelijkheden bij de Stad te publiceren;
Personeelsactiviteiten	g) foto's of video's van personeelsactiviteiten te posten zonder expliciete toestemming van de afgebeelde personen.

Artikel 17.

Het personeelslid moet zich er van bewust worden dat zodra hij of zij content op openbare websites plaatst hierover geen controle meer kan uitgeoefend worden, en het aantal personen die deze content gewaarworden of verder verspreiden niet meer kan ingeperkt worden, waardoor het een openbaar karakter krijgt en het niet langer beschermd is als privé-communicatie.

Elk personeelslid is persoonlijk aansprakelijk voor de inhoud die hij of zij op openbare websites publiceert.

HOOFDSTUK V. COMPUTER- EN INFORMATIEBEVEILIGING.

Artikel 18.

Het personeelslid doet mee aan de beveiliging van het informatiesysteem door in het bijzonder de volgende principes na te leven:

Integriteit	a) de herkomst en onschadelijkheid van bezochte websites en inkomend berichtenverkeer te verifiëren; b) het openen van spammails en onbetrouwbare bijlagen, alsook het downloaden van onbetrouwbare bestanden, zo veel mogelijk te voorkomen; c) te vermijden om te klikken op links in dergelijke onbetrouwbare mails, websites en bestanden; d) spam te rapporteren via de ter beschikking gestelde middelen (https://intranet.brussel.be/e-mail-alarm);
Paswoorden en – beveiliging	e) een paswoord te kiezen dat niet gemakkelijk te raden is, en deze regelmatig te veranderen, en dat conform is met de paswoordpolicy; f) gebruik te maken van de dubbele authenticatie (MFA) in functie van de ter beschikking gestelde middelen;
Toegang tot de werkpost	g) bij het verlaten van zijn werkpost toegang tot zijn of haar computer en andere apparaten te vergrendelen;
Opslag	h) netwerklocaties te gebruiken voor de opslag van professionele bestanden in plaats van de harde schijf, tenzij het gaat over voorbereidende documenten; i) rekening te houden met het feit dat van de lokale schijf geen back-up gemaakt wordt.

Artikel 19.

Het is voor het personeelslid verboden

Paswoorden	a) zijn of haar paswoord te delen met anderen, zowel personeelsleden van de Stad als buitenstaanders (ICT-dienstverlener, consultants, vrienden, familie, …); b) het paswoord van een collega te vragen, ontvangen of gebruiken; c) een paswoord fysiek of digitaal te noteren; d) hetzelfde paswoord te gebruiken voor zowel aan het beroep verbonden accounts als voor privéaccounts;
Toegang accounts	e) anderen, intern of extern, toegang te geven tot zijn of haar account; f) toegang tot de account van een collega te vragen, ontvangen of gebruiken;
Misbruik, sabotage of vandalisme	g) om misbruik te maken van ontdekte kwetsbaarheden in het systeem; h) om schade toe te brengen aan hardware, software, bestanden of processen, intern of extern, of deze ongeoorloofd te wijzigen of te verwijderen; i) om gegevens onderworpen aan de rechten van anderen of persoonsgegevens die niet noodzakelijk zijn voor de functie te raadplegen; j) om te verzwijgen dat men toegang heeft tot gegevens die normaal niet toegankelijk zijn;
Software	k) om niet toegestane software te installeren of te gebruiken, d.i. software zonder de voorafgaande schriftelijke toelating van een meerdere of software die niet bedoeld is voor het uitoefenen van beroepsactiviteiten (bijvoorbeeld: gratis online tool); l) willens en wetens uitvoerbare bestanden (bv. ".exe") te activeren behalve met goedkeuring van de ICT-dienstverlener;
Hardware	m) om verwijderbare media aan te sluiten (USB-stick, smartphones, externe harddisk,…) tenzij de herkomst en inhoud gekend is ; n) hardware materiaal dat niet ter beschikking werd gesteld door I-City, te verbinden met de computer, met uitzondering van randapparatuur die geen software installatie vereist (toetsenbord, muis, scherm, bluetooth headset…) en waarvoor het onderhoud niet wordt voorzien door I-City ;
Opslag	o) om werkgerelateerde bestanden op te slaan in clouddiensten die niet door de stad werden voorzien (Dropbox, …) p) om aan het werk gerelateerde gegevens op te slaan op een privéadres; q) om bestanden te verwijderen op gedeelde dossiers zonder expliciete goedkeuring van de eigenaar van het document (+ motivering waarom het document verwijderd moet worden);
Werken vanop afstand	r) zijn of haar pc en andere mobile devices onbewaakt en/of onvergrendeld achter te laten, in het bijzonder waar deze het doelwit van diefstal kunnen worden; s) om in publieke ruimtes om te gaan met vertrouwelijke informatie (bv. tegen meelezen); t) om afgedrukte pagina's met vertrouwelijke informatie mee naar huis te nemen, omdat deze moeilijk te beveiligen zijn.

HOOFDSTUK VI. VERANTWOORDELIJKHEID VAN HET PERSONEELSLID.

Artikel 20.

In geval van niet-naleving van de bepalingen van voorliggende policy kan het personeelslid aansprakelijk worden gesteld volgens de regels inzake de wettelijke aansprakelijkheid van personeelsleden (grove nalatigheid of herhaalde lichte nalatigheid).

Naast de wettelijke aansprakelijkheid kan niet-naleving van de bepalingen van deze overeenkomst leiden tot disciplinaire maatregelen.

Bij wijze van voorbeeld, deze niet-exhaustieve lijst, waarbij zowel tijdens als buiten de werkuren, sprake kan zijn van een ernstige fout :

- elke opzettelijke schending van de geheimhoudingsplicht (bv. verspreiding van gegevens onderworpen aan de rechten van anderen of persoonsgegevens, ongeoorloofde toegang tot professionele inhoud)
- elke inbreuk op de Deontologische Code, met name de publicatie van hatelijke, lasterlijke of laakbare commentaren op openbare websites. Publicatietypes die worden beschouwd als strijdig met de Deontologische Code:
    - laakbare pornografische aard is, zoals kinderporno of beelden;
    - racistisch of haatdragend jegens buitenlanders ;
    - discriminerend op basis van geslacht, seksuele geaardheid, handicap, geloof, filosofische of politieke overtuigingen;
    - revisionistisch;
    - pestgedrag of ongewenste intimiteiten bevattend of bevorderend;
    - respectloos ten opzichte van anderen ;
    - of in strijd met de goede zeden of de waardigheid van anderen aantast;
- Elk gedrag dat opzettelijk de veiligheid van het informatiesysteem ondermijnt (bijvoorbeeld hacken).

Deze bepaling belet eventuele strafrechtelijke aansprakelijkheid van het personeelslid bij oneigenlijk gebruik van ICT-middelen niet.

Artikel 21.

In geval van gedrag dat de veiligheid van het informatiesysteem in gevaar brengt, behoudt de werkgever zich het recht voor het personeelslid met onmiddellijke ingang de toegang tot zijn/haar account te ontzeggen.

Artikel 22.

Van het personeelslid wordt verwacht kennis te nemen van de totaliteit van deze policy en deze na te leven.

Het personeelslid wordt door zijn of haar meerdere, of bij het aanwerven, gevraagd een kennisneming te ondertekenen.

Artikel 23.

Deze policy moet steeds worden geïnterpreteerd en toegepast met het oog op de goede werking van de diensten van de Stad en op de veiligheid van en zorg voor de ICT-middelen en netwerken van de Stad.

In het geval het personeelslid na het doornemen van deze policy niet zeker is of twijfelt over wat acceptabel gebruik van de ICT-middelen is, wat hij of zij niet mag doen of welke veiligheidsmaatregelen hij of zij moet nemen om de integriteit van het informaticasysteem niet aan te tasten, is deze verplicht om begeleiding en verduidelijking te vragen aan zijn of haar directie of (adjunct-)informaticacorrespondent.

Artikel 24.

Het personeelslid is verplicht, bij het vaststellen van een IT-incident qua computer- en informatieveiligheid in het kader van deze policy, onmiddellijk melding hiervan te maken aan de CISO (via security@brucity.be) om verdere schade en verdere incidenten te vermijden. Dit zowel met betrekking tot zichzelf als tot zijn of haar medewerkers en werkomgeving. Het personeelslid wordt aangespoord op dat moment niets verder te ondernemen tot hij of zij toelating hiervoor gekregen heeft.

Artikel 25.

Indien een personeelslid kennis krijgt van een incident in verband met persoonsgegevens (verlies van vertrouwelijkheid, integriteit of beschikbaarheid van persoonsgegevens), moet hij/zij onmiddellijk de DPO informeren op DPO@brucity.be.

Artikel 26.

Overtreding van de bepalingen van deze policy kan leiden tot disciplinaire procedures en sancties.

HOOFDSTUK VII. PRIVACY VAN HET PERSONEELSLID.

Sectie 1 - BESCHERMING VAN PERSONEELSGEGEVENS

Artikel 27.

De gegevensverwerkingen betreffende het personeelslid worden beschreven in het beschikbare Privacy charter inzake de bescherming van gegevens van de personeelsleden van de Stad Brussel. De Stad verwerkt de gegevens van haar personeelsleden in overeenstemming met hun recht op privacy, waaronder de AVG en/of de Privacywet.

De Stad hecht veel belang aan de eerbiediging van de persoonlijke levenssfeer van haar personeelsleden en leeft de Privacywet nauwgezet na. Wanneer zij besluit controles uit te voeren, verbindt zij zich ertoe dit te doen in overeenstemming met de door deze wet voorgeschreven beginselen van finaliteit, proportionaliteit en transparantie.

Sectie 2 - CONTROLEPROCEDURE VOOR HET GEBRUIK VAN ICT-MIDDELEN DOOR PERSONEELSLEDEN

Artikel 28.

Globale controle: de stad kan een systematische en globale controle op het gebruik van een professionele toepassing uitvoeren. Dit toezicht moet echter voldoen aan de beginselen van CTT 81 en de aanbevelingen met betrekking tot de recht aan de persoonlijke levenssfeer.

Elke systematische controle op het gebruik van ICT-middelen of -toepassingen die ter

beschikking van het personeel worden gesteld, moet het voorwerp uitmaken van een specifiek reglement dat via een overlegprocedure inclusief het DPO wordt gevalideerd. Deze regels moeten in het bijzonder de volgende beschermingsmaatregelen bevatten :

A) Finaliteitsbeginsel

De controle op het gebruik van de ICT-middelen kan enkel plaatsvinden indien een of meerdere van de volgende finaliteiten worden nagestreefd:

- de veiligheid en/of het goede werken van de informaticasystemen, alsook de materiele bescherming van het materiaal;
- het voorkomen van daden die onwettig of in strijd met de goede zeden zijn of de waardigheid van anderen aantasten;
- het eerbaar naleven van de gebruiksrichtlijnen betreffende de ICT-middelen zoals vermeld in dit document;
- de bescherming van de reputatie en de sociale en economische interesses van de Stad en haar instituties;
- de bescherming van de privacy, de waardigheid en de reputatie van haar personeelsleden en zakenpartners;
- de bescherming van de privacy van de burgers.

B) Transparentiebeginsel: voorafgaande collectieve of individuele informatie van personeelsleden. Deze informatie specificeert de procedures, het doel en de duur van de controle, evenals eventuele sancties.

C) Proportionaliteitbeginsel: de controle mag niet systematisch gebeuren noch oneindig zijn maar moet beperkt blijven tot de tijd die nodig is om het nagestreefde doel te bereiken.

D) Individualiseringbeginsel

De Stad weerhoudt zich het recht om, in het kader van de finaliteiten en de procedure hierboven beschreven, over te gaan tot de identificatie van het betrokken personeelslid. Deze controle kan louter resulteren in de identificatie van een personeelslid indien zij tot doel heeft:

- het voorkomen van daden die onwettig of in strijd zijn met de goede zeden of daden de waardigheid van anderen aantasten;
- de economische en financiële belangen van de Stad te beschermen;
- de veiligheid of de werking van de computersystemen te verzekeren;
- elke andere inbreuk op de veiligheidsvoorschriften stop te zetten.

In andere gevallen, zoals bv. een inbreuk op de naleving van de gebruiksregels van ICT-middelen, kan een identificatie enkel plaatsvinden nadat eerst het personeel gezamenlijk gewaarschuwd werd dat een van deze regels overtreden werd en een gelijkaardige overtreding opnieuw heeft plaatsgevonden.

Artikel 29. Uitzonderlijke controles

Op het moment dat een herhaald misbruik of verboden verbruik, d.i. een inbreuk op de veiligheidsmaatregelen en gebruiksrichtlijnen aangehaald in deze policy, wordt vermoed, bijvoorbeeld op basis van toevallig ontdekt bewijs, kan het departementshoofd, hieronder genoemd de aanvrager van de controle, de DPO inlichten. Hierbij vermeldt hij expliciet en schriftelijk welk herhaald misbruik of verboden verbruik wordt vermoed.

De DPO geeft een onafhankelijk oordeel over de rechtmatigheid, evenredigheid, noodzaak en wettigheid van de controle. Dit advies geeft aan welke privacybeschermingsmaatregelen moeten worden nageleefd als onderdeel van de controle.

Enkel de Stadssecretaris kan beslissen om een verder onderzoek in te richten en het gebruik van de ICT-middelen te monitoren.

Het onderzoek heeft alleen tot doel bewijs te zoeken voor de feiten waarover wordt geklaagd en mag in geen geval leiden tot een uitgebreidere controle dan de aanvankelijk gevraagde controle.

De Stad laat controles enkel in het kader van de beginselen beschreven in deze ICT-policy uitvoeren en maakt in elk geval niet op permanente wijze gebruik van deze capaciteiten en voert geen voortdurende en systematische controles uit op het personeelslid.

Het personeelslid waarop een controle betrekking heeft, wordt van de controle op de hoogte gesteld voordat deze wordt uitgevoerd.

De hierboven beschreven controle heeft geen betrekking op de niet-naleving van de bepalingen die in dit beleid als aanbevelingen en goede praktijken worden beschreven.

Artikel 30.

De verantwoordelijke van de uitvoering van deze controle is de ICT-dienstverlener. Deze heeft o.a. de technische capaciteit

- om een algemene lijst op te roepen van alle bezochte internetwebsites via haar netwerk, alsook de duur van het bezoek en het moment waarop dit bezoek plaatsvond;
- om betreffende het e-mailverkeer zaken zoals de frequentie, het aantal, de grootte, de bijlagen, … te monitoren;
- om per telefoon de communicatiegegevens te bekijken zoals deze gefactureerd werden;

De ICT-dienstverlener houdt zich aan een vertrouwelijke afhandeling van de gegevens en deze kunnen worden bewaard gedurende het onderzoek of de tijd noodzakelijk voor het verloop van een gerechtelijke procedure.

Op het moment dat de ICT-dienstverlener een afwijking vaststelt, informeert deze de DPO. Onder afwijking wordt verstaan elke inbreuk op de richtlijnen van deze policy. De afwijkingen worden formeel door de aanvrager van de controle vastgesteld, die een schriftelijk rapport opstelt.

Artikel 31.

De Stad weerhoudt zich het recht om, in het kader van de finaliteiten en de procedure hierboven beschreven, over te gaan tot de identificatie van het betrokken personeelslid. Deze controle kan louter resulteren in de identificatie van een personeelslid indien zij tot doel heeft:

- daden die onwettig of in strijd zijn met de goede zeden of de waardigheid van anderen aantasten te voorkomen;
- de economische en financiële belangen van de Stad te beschermen;
- de veiligheid of de werking van de computersystemen te verzekeren;
- elke andere inbreuk op de veiligheidsvoorschriften stop te zetten.

In andere gevallen, zoals bv. een inbreuk op de naleving van de gebruiksregels van ICT-middelen, kan een identificatie enkel plaatsvinden nadat eerst het personeel gezamenlijk gewaarschuwd werd dat een van deze regels overtreden werd, en een gelijkaardige overtreding opnieuw heeft plaatsgevonden.

Artikel 32.

Het betreffende personeelslid heeft het recht om

- alle informatie te ontvangen betreffende deze controle bij de DPO (**recht op inzage en recht op informatie**);
- deze informatie door de DPO te laten vernietigen of corrigeren in het geval dat deze incorrect bleek of in strijd met de regelgeving van deze policy werd vastgelegd of meer dan één jaar oud is (**recht op verbetering en recht op gegevens wissing)**;
- tot een maand na het ingelicht worden van de controle bezwaar te maken tegen deze controle bij de Stadssecretaris (**recht op bezwaar**) of om opschorting van de controle te verzoeken voor zover deze in strijd is met de geldende wetgeving (**recht op beperking**).
- Een geautomatiseerd besluit dat in het kader van de controle is genomen, aan te vechten en menselijke tussenkomst in het besluit te eisen (**recht om niet te worden onderworpen aan een geautomatiseerd besluit**).
- Als uitzondering op artikel 20§3 van de AVG, hebben personeelsleden het recht om controlegegevens met betrekking tot de arbeidsrelatie te verkrijgen in een gestructureerd, algemeen gebruikt en machine leesbaar formaat en het recht om deze gegevens aan een andere verwerkingsverantwoordelijke te verstrekken zonder dat de Stad hiertegen bezwaar maakt (**recht op overdraagbaarheid**).

Al deze aanvragen kunnen worden gericht aan de DPO.

HOOFDSTUK VIII. KWALITEITSTOEZICHT.

Artikel 33.

Een evaluatie van deze policy zal regelmatig worden gerealiseerd om bovenstaande richtlijnen te herzien in functie van

- nieuwe communicatiemiddelen en technologieën die gebruikt worden door de personeelsleden van de Stad;
- een evolutie van het wettelijk kader;
- het toetsen van de uitwerking en efficiëntie van de controleprocedures;
- in Functie van het voor een andere reden noodzakelijk geacht wordt door de werkgever of andere belanghebbenden.