POLITIQUE ICT

Directives concernant les moyens ICT

Table des matières

CHAPITRE I. OBJET ET PORTÉE.

Introduction

La présente politique a pour but :

- d'informer le personnel à propos de l'utilisation des moyens ICT mis à disposition et de l'inciter à les exploiter pleinement ;
- de garantir l'intégrité du système informatique de la Ville ;
- de protéger les données qui sont sous la responsabilité de la Ville, ou qui ont trait à la vie privée des membres du personnel ou de citoyens, et de garantir leur vie privée, conformément au droit à la vie privée ;
- de protéger la réputation en ligne de la Ville d'un éventuel comportement abusif d'un membre du personnel sur les espaces en ligne publics ;
- d'encadrer le contrôle de l'usage des moyens ICT par les membres du personnel.

Les membres du personnel ont généralement une adresse e-mail professionnelle, accès à Internet, à la téléphonie et à la communication électronique, depuis un poste de travail fixe ou leur poste de travail mobile. Le présent document représente le point de vue de la Ville concernant l'utilisation de l'Internet et des moyens ICT de ses membres du personnel, ainsi que le contrôle de cet usage dans le respect de la vie privée. La violation des présentes directives peut donner lieu à des sanctions disciplinaires.

Article 1. Concepts

Les concepts suivants, utilisés à plusieurs reprises dans la présente politique, sont définis comme suit :

Le membre du personnel	Tout membre du personnel de la Ville, quelle que soit la nature juridique du lien avec l'employeur (membre du personnel sous statut ou sous le couvert d'un contrat de travail, membre du cabinet, stagiaire, membre du personnel détaché à la Ville...). N'est pas inclus : le personnel enseignant de l'Enseignement public de la Ville.
L'employeur	La Ville et ses représentants auxquels le membre du personnel est lié par le biais d'un contrat de travail ou d'un statut.
La politique	Le présent document et toutes ses directives.
Moyens ICT	Un vaste concept qui englobe tout ce que le membre du personnel utilise pour se connecter à l'Internet ou au réseau, ou pour communiquer, que ce soit par voie matérielle ou numérique, électronique ou téléphonique, et en particulier les ordinateurs fixes, les ordinateurs portables, les imprimantes, les téléphonesfixes et les appareils mobiles (tablettes, smartphones, PDA...).
La donnée	Tout ce qui peut être sauvegardé et classé, sur papier ou au format numérique, en lettres et en chiffres ou au format vidéo ou audio.
Données à caractère personnel	« toute information se rapportant à une personne physique identifiée ou identifiable (…) ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale » article 4 RGPD.

Données soumises à droit d'autrui	Les données soumises à droit d'autrui sont des données qui, en fonction de leur nature, - sont uniquement destinées à un usage interne, - peuvent uniquement être consultées par quelques personnes habilitées, - ou qui sont protégées par la loi (notamment le secret d'entreprise ou la propriété intellectuelle)
RGPD	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE **(règlement général sur la protection des données)**
Loi sur la vie privée	La loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.
Le fichier	Ensemble de données (informatiques) ordonnées, comme un document detraitement de texte, des dépliants, des illustrations...
Espaces publics en ligne	Toute forme de communication publique sur l'Internet. Quelques exemples (attention, cette liste n'est pas exhaustive) : sites et applications de réseaux sociaux (Facebook, Snapchat, LinkedIn…), sites de partage de vidéos et photos (Youtube, Instagram…), blogs, forums ou groupes de discussion (Reddit, Google Groups…), chatrooms, sites Web de messagescourts (Twitter…), sites Web de publication de contenu (Wikipédia…)…

Data Protection Officer (DPO)	La personne indépendante qui donne des avis et aide à la mise en en œuvre des régimes en matière de vie privée, y compris de la protection des données. « 1. Les missions du délégué à la protection des données sont au moins les suivantes: a) informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du présent règlement et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données; b) contrôler le respect du présent règlement, d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant; c) dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution (…); d) coopérer avec l'autorité de contrôle; e) faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36 (du RGPD), et mener des consultations, le cas échéant, sur tout autre sujet. 2. Le délégué à la protection des données tient dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement. » article 39 RGPD Joignable via privacy@brucity.be
Chief Information Security Officer (CISO)	La personne qui établit les stratégies en matière de Sécurité du Système d'Information et évalue la sécurité de ce système en vue de son amélioration. Joignable via security@brucity.be
Prestataire de services ICT	Celui qui met à disposition les moyens ICT ou les exploite dans le cadre d'une relation contractuelle avec la Ville.

CHAPITRE II. MISE A DISPOSITION DE MOYENS ICT.

Article 2.

Plusieurs moyens ICT standards sont mis à la disposition de chaque membre du personnel de la Ville en fonction de leur position, avec un usage privatif comme avantage en toute nature. Ces moyens restent la propriété de l'employeur. Le membre du personnel a l'obligation de prendre soin de ces moyens.

Pour ce qui concerne spécifiquement la mise à disposition de moyens de téléphonie mobile, le collaborateur se référera aussi à la « politique de téléphonie mobile de la Ville », disponible sur l'intranet, et qui est complémentaire à la présente politique ICT

Le membre du personnel restitue ces moyens en cas d'arrivée à expiration ou de cessation de son occupation, ainsi que tout le matériel connexe (sacs, étuis...), à son

correspondant informatique (adjoint) ou en son absence au secrétariat central, et ce au plus tard lors du dernier jour presté.

En cas de vol de matériel, le membre du personnel sera tenu d'en faire la déclaration à la police, de remettre le procès-verbal au service desk d'i-City et d'informer au plus vite le DPO à l'adresse dpo@brucity.be

Article 3.

Plusieurs moyens ICT sont mis en commun à disposition de tout ou partie du personnel. Le membre du personnel est également tenu de s'en occuper en personne prudente et raisonnable et en respect de la présente politique.

Article 4.

L'employeur se réserve le droit d'interdire à tout moment et sans avertissement l'accès à certains sites Web ou fichiers, pour préserver la sécurité du système informatique en général, ou pour empêcher l'une des activités interdites mentionnées dans la présente politique.

Article 5.

Fin de la mise à disposition : tous les moyens ICT que l'employeur met à la disposition de ses membres du personnel restent la propriété de la Ville. Toutes les données émises, reçues et/ou conservées dans des dossiers, fichiers et/ou e-mails sont et restent la propriété de la ville, sauf si elles sont clairement qualifiées de personnelles (voir chapitre III, Section II : Usage privé).

Après le départ du membre du personnel, la Ville se réserve le droit d'accéder aux données professionnelles du dit membre, ainsi qu'à ses courriers électroniques professionnels, dans la mesure où un tel accès est absolument nécessaire :

(1) à la continuité d'un service ou de la fonction dans la mesure où l'interruption du dit service ou de la fonction porterait préjudice à la Ville ou à des tiers de manière disproportionnée,

(2) à la résolution d'un problème impérieux tel que la sécurité du système d'information ou la sécurité d'un tiers.

L'accès est soumis à un avis motivé du DPO et un accord du Secrétaire Communal. Un tel accès ne concernera que les données nécessaires à la continuité du service ou de la fonction et ne pourra concerner les données ou mails identifiés comme personnels conformément à l'article 9. Cette accès ne pourra avoir lieu que dans un délai maximum de 3 mois après la fin de la collaboration. Après ce délai, les données et mails seront supprimés.

En tout état de cause, la continuité du service ou de la fonction sera considérée comme accomplie dans la mesure où le membre du personnel organise la transmission des données et mails utiles à la continuité du service ou de la fonction avant son départ.

Cet article n'entre pas en contradiction avec les éventuelles consultations réalisées dans un cadre légal, notamment en cas de procédure judiciaire.

CHAPITRE III. UTILISATION DES MOYENS ICT DANS LE CADRE DU TRAVAIL

Article 6.

Toutes les directives suivantes concernant l'utilisation s'appliquent à tous les moyens

mis à disposition,ainsi qu'aux moyens ICT propres lorsque le membre du personnel les utilise dans le cadre de son travail et pendant les heures de travail (ordinateur privé via VPN, smartphone propre...).

Le membre du personnel qui travaille à distance est soumis aux mêmes directives que s'il se trouve sur le lieu de travail normal.

Une utilisation des moyens ICT dans le cadre du travail concerne aussi bien l'utilisation pendant les horaires de temps de travail, une utilisation en tout temps sur les applications professionnelles fournies par la Ville, une utilisation sur le réseau internet de la Ville.

Section 1 - USAGE PROFESSIONNEL.

Article 7.

Pour les directives concernant un usage professionnel des moyens ICT, la direction peut imposer des exigences plus strictes. Il est attendu du membre du personnel de respecter les bonnes pratiques suivantes dans la mesure du possible :

Corres-pondance	a) utiliser une adresse e-mail officielle (par ex. sous le domaine brucity.be) pour toute correspondance, interne ou avec des externes dans le cadre de sa fonction ; b) consulter régulièrement son courrier entrant, y répondre à temps et éventuellement indiquer le délai dans lequel une suite pourra être donnée au message ; c) limiter au nécessaire absolu le nombre de destinataires dans les e-mails ; d) ne qualifier un message d'urgent que si c'est vraiment nécessaire ; e) en cas d'envoi erroné d'un e-mail, tenter de rappeler cet e-mail ou d'informer le mauvais destinataire de son erreur ; f) en cas de notification de rappel d'un e-mail, ne pas l'ouvrir et le supprimer directement ;
Signature et police de caractères	g) utiliser la signature d'e-mail et la police de caractères standardisées fixées par la cellule Communication et disponibles dans la charte graphique ;
Out of office	h) en cas d'absence de plus d'un jour, rédiger un message d'absence de bureau - ce message fait mention de la période d'absence ainsi que de la ou des personnes ou du service à contacter en cas d'urgence ;
Annexes d'e-mails	i) éviter de joindre des fichiers volumineux en annexe à des e-mails ; j) faire référence à un dossier partagé au lieu de joindre des fichiers à des e-mails ;
Imprimer	k) éviter tant que possible l'impression d'e-mails et de documents et d'accorder la préférence à leur projection et transmission par voie numérique ; l) n'imprimer des documents contenant des données soumises à droit d'autrui ou à caractère personnel que lorsque c'est absolument nécessaire ou légalement obligatoire ;
Archiver	m) respecter les recommandations de la Ville en matière d'archivage, et à défaut de : • régulièrement nettoyer sa messagerie et n'y conserver que les messages

	pouvant encore servir dans la mesure où ils n'ont pas encore été archivés ; • archiver sa messagerie avant de supprimer des messages et fichiers importants ;
Calendrier	n) indiquer toutes ses indisponibilités dans son calendrier Outlook ;
Durabilité	o) éteindre ses appareils (écrans, PC...) en quittant le poste de travail, ainsi que les appareils partagés (imprimantes, tableaux électroniques...) s'il est le dernier à quitter le lieu de travail.

Article 8.

Un disclaimer est automatiquement ajouté aux envois adressés à des domaines qui ne sont pas directement liés à la Ville de Bruxelles ou à son prestataire de services ICT. Le membre dupersonnel ne peut en aucun cas le modifier.

Article 9.

L'envoi de messages collectifs à tous les membres de plusieurs départements ou à l'ensemble du personnel de la Ville est soumis à une procédure particulière :

Demande	a) Les demandes d'envoi sont à transmettre à l'adresse e-mail du service Communication interne du département RH, qui vérifiera si, en fonction de ce qui suit, rien ne fait obstacle à la diffusion de ce message. La diffusion aux membres du personnel qui n'ont pas facilement accès à leur adresse e-mail doit également être assurée, sous la responsabilité de leur dirigeant. b) Les textes qui sont soumis seront approuvés par le département/cabinet concerné. Les coordonnées de l'éditeur responsable (service ou personne) seront mentionnées, avec l'adresse e-mail. c) Pour les messages des catégories 2 à 4, les textes doivent être transmis largement à l'avance pour permettre au service Communication interne de s'occuper de la mise en page et de l'envoi. Un délai minimum de deux jours est requis
Catégories	d) Les messages seront classés par importance (exemples) : CAT 1: Organisation du travail = coupures de courant, interventions techniques et travaux de maintenance au réseau, à la téléphonie, modifications du règlement ; CAT 2 : Offres d'emploi = appels à la mobilité, recrutement, Selor, formations … ; CAT 3: Invitation gratuite ou avantage pour le personnel de la Ville ; CAT 4: Événement = publicité pure (aucun avantage pour les membres du personnel).
Contenu	e) Le demandeur limitera le texte à 250 mots par langue. Des liens vers l'intranet et Internet sont autorisés. f) Dans les messages, les noms des échevins seront remplacés par « Le Collège ».
Bilinguisme	g) Un bilinguisme total (français/néerlandais) est de rigueur, tant dans le texte du message que dans les éventuelles annexes (.pdf, image avec texte...). Compte tenu de la législation relative à l'usage des langues, le demandeur fournira également les liens dans les deux langues en cas de référence vers des sites Web (de la Ville ou autres).

Annexes	h) Les éventuelles annexes doivent être fournies dans les formats les plus courants, comme .jpg (dessin ou photo), .doc (Word), .xls (Excel), .pdf (Acrobat), et il ne peut en aucun cas s'agir de documents scannés.
Diffusion	i) En présence de différentes demandes introduites simultanément, le service Communication interne du département RH pourra décider de l'ordre d'envoi, afin d'éviter de dépasser la fréquence d'un message par jour. j) Sauf mention contraire, la diffusion se fera à l'ensemble des membres du personnel de la Ville. Sur demande, l'envoi peut également être plus ciblé,tant qu'il vise des groupes ou listes prévus en Outlook, comme « Collège », « Départements »...
Suspension, adaptation ou refus.	k) Les e-mails qui sont envoyés tardivement ou qui ne sont pas conformes aux dispositions du présent règlement peuvent être envoyés plus tard par le Service Communication interne du département RH. Ce Service peut également demander d'adapter l'e-mail au règlement et, en cas de défaut, refuser l'envoi de l'e-mail.
Aucune deviation	l) Il est interdit d'envoyer ce type de messages d'une autre manière.

Section 2 - USAGE PRIVÉ.

Article 10.

Conformément aux législations fédérales en vigueur, l'usage privatif en dehors de la journée de travail est inhérent à la possession d'un laptop et représente un avantage de toute nature.

En tout état de cause, l'usage privatif des moyens ICT dans le cadre du travail n'est pas autorisé s'il :

a) est fréquent et de longue durée ;
b) a un impact sur les obligations du membre du personnel ou ses collaborateurs ;
c) a un impact sur le fonctionnement de la Ville ;
d) induit des frais supplémentaires pour la Ville ;
e) contrevient aux autres articles de la présente politique ;
f) contrevient au RGPD et/ou à la loi sur la vie privée.

Voici, à titre d'information, quelques exemples d'usage personnel autorisé :	- exécuter une transaction bancaire en ligne simple ; - rédiger un court e-mail personnel ; - mener un bref entretien téléphonique ; - imprimer sur une base exceptionnelle quelques pages à usage privé.
Voici, à titre d'information, quelques exemples d'usage personnel non autorisé :	- remplir des documents électroniques à des fins privées de manière exhaustive ; - copier ou imprimer un livre ; - téléphoner à l'étranger ; - faire des recherches personnelles dans des applications professionnelles ; - diffuser des chaînes de lettres, jouer à des jeux, passer du temps dans des chatrooms en ligne et autres ; - écouter longtemps et en streaming de la musique et/ou des vidéos qui ne s'inscrivent pas dans le cadre du travail ;

- télécharger des fichiers volumineux ;
- s'engager dans des activités personnelles à but commercial ou faire de la publicité d'intérêts étrangers à ceux de la Ville

Article 11.

L'usage privé de l'adresse e-mail professionnelle est autorisé lorsque le membre du personnel qualifie les e-mails sortants de personnels[1] et ajoute ce qui suit au message : « le contenu de ce message est personnel et ne peut en aucun cas impliquer la responsabilité de la Ville ».

Les e-mails revêtant un caractère personnel doivent également être conservés dans un dossier Outlook « privé » s'ils ne peuvent être consultés par la Ville.

Tout e-mail non qualifié comme personnel sera considéré comme un mail professionnel, ce qui peut impliquer un accès à cet e-mail en cas de récupération conformément à l'article 5.

Article 12.

Des données privées ne peuvent être sauvegardées que dans un dossier nommé « privé » sur le disque local (disque dur du PC) si elles ne peuvent être consultées par la Ville. Ce dossier ne peut contenir aucune donnée professionnelle. En cas de cessation ou arrivée à expiration du contrat et/ou de restitution des moyens ICT, le membre du personnel est tenu de récupérer lui-même ses données privées avant de la fin de la collaboration, ce après quoi elles seront automatiquement supprimées.

Section 3 - USAGE INTERDIT SUR LE RÉSEAU DE LA VILLE

Article 13.

Aucun membre du personnel ne peut visiter des sites Web, envoyer ou répondre à des messages dont le contenu :

- est de nature érotique ou pornographique
- est raciste ou haineux envers les étrangers ;
- est discriminant sur la base du genre, de l'orientation sexuelle, du handicap, de la croyance, de convictions philosophiques ou politiques ;
- est révisionniste ;
- contient ou favorise un comportement de harcèlement moral ou sexuel ;
- est irrespectueux vis-à-vis d'autrui ;
- ou est de toute autre manière contraire aux bonnes mœurs, ou nuit à la dignité d'autrui ;

[1] Rendez-vous pour ce faire dans Outlook, sous « Options », « Message settings ». Sélectionnez « Personal »sous « Sensitivity » ou ajoutez « privé » dans le titre du message.

CHAPITRE IV. UTILISATION DES MOYENS ICT, Y COMPRIS EN DEHORS DU CADRE DU TRAVAIL

Section 1 - USAGE PRÉJUDICIABLE POUR LA VILLE

Article 14.

Aucun membre du personnel ne peut, même en dehors des heures de travail :

Usage illégal	a) s'engager dans toute forme de fraude, piraterie, paris en ligne, vente de stupéfiants, infraction aux droits d'auteur... ou toute autre activité illégale ;
Diffusion de données soumises à droit d'autrui et de données à caractère personnel	b) diffuser des données soumises à droit d'autrui concernant la Ville, ses établissements, membres du personnel, services, partenaires commerciaux, clients ou autres intéressés, sauf dans le cadre de ses obligations ; c) faire une recherche dans les données soumises à droit d'autrui ou dans les données à caractère personnel des applications de la Ville à des fins personnelles ; d) accéder à ou communiquer des données soumises à droit d'autrui ou à caractère personnel de manière non autorisée ; e) partager à des tiers, même dans des communications privées, des données soumises à droit d'autrui ou à caractère personnel ;
Calomnie	f) calomnier la Ville, ses établissements, services, membres du personnel, partenaires commerciaux, clients ou autres intéressés ;
Diffusion de l'opinion propre	g) utiliser la signature officielle dans des correspondances privées ; h) faire passer des opinions propres pour des opinions officielles de la Ville, ou parler de manière non autorisée en son nom.

Section 2 - CONCERNANT LES ESPACES PUBLICS EN LIGNE

Article 15.

Des règles spécifiques relatives à l'usage professionnel - c'est-à-dire applicables aux collaborateurs qui sont habilités à s'exprimer au nom de la Ville ou à représenter la Ville sur les réseaux sociaux - sont gérées par les services Communication et ne font pas partie de la présente politique.

Dans tous les cas, les membres du personnel qui ne disposent pas d'une telle autorisation ne peuvent s'adonner à des activités sur les réseaux sociaux en se faisant passer pour la Ville ou en agissant au nom de la Ville. Ils sont cependant autorisés à indiquer la Ville comme employeur sur leur compte, en indiquant toutefois qu'il s'agit d'un compte personnel. Ils sont également autorisés à partager des messages publiés sur les comptes officiels de la Ville.

Article 16.

Toutes les dispositions de la présente politique concernant l'utilisation de moyens ICT s'appliquent également à l'utilisation des espaces publics en ligne (réseaux sociaux, forums…) sur le lieu de travail ou en déplacement dans le cadre du travail ou du télétravail.

Quoi qu'il en soit, lorsque le collaborateur de la Ville se rend sur les réseaux sociaux, même à partir de moyens ICT personnels et en dehors des heures de travail, il lui est à tout moment interdit de :

Contenu contraire à la déontologie	a) publier ou interagir de manière publique sur du contenu : i. de nature pornographique répréhensible, tel que la pédopornographie ou des captures d'agressions sexuelles ; ii. raciste ou haineux envers les étrangers ; iii. discriminant sur la base du genre, de l'orientation sexuelle, du handicap, de la croyance, de convictions philosophiques ou politiques ; iv. révisionniste ; v. contenant ou favorisant un comportement de harcèlement moral ou sexuel ; vi. de tout autre manière contraire aux bonnes mœurs, ou nuit à la dignité d'autrui
Données soumises à droit d'autrui et/ou données à caractère personnel	b) diffuser des données soumises à droit d'autrui ou à caractère personnel concernant la Ville, ses établissements, membres du personnel, services, partenaires commerciaux,clients ou autres intéressés
Calomnie	c) calomnier la Ville, ses établissements, membres du personnel, services;
Données inexactes	d) publier des déclarations mensongères, trompeuses ou source de confusion concernant la Ville, ses établissements, membres du personnel, services, partenaires commerciaux et autres intéressés ; e) se prononcer pour une autre personne qui est liée à la Ville; f) de publier des informations erronées concernant son expérience ou ses responsabilités professionnelles au sein de la Ville;
Activités du personnel	g) de publier des photos ou vidéos d'activités du personnel sans consentement explicite des personnes représentées.

Article 17.

Le membre du personnel doit avoir conscience du fait que dès qu'il publie du contenu sur les réseaux sociaux, ce dernier échappe à son contrôle, et que le nombre de personnes pouvant prendre connaissance de ce contenu ou le diffuser ne peut plus être limité, dès lors il revêt un caractère public et n'est plus protégé comme communication privée. L'accès par l'employeur aux contenus publiés sur les espaces publics en ligne n'est pas prohibé et toute publication contraire à l'article 16 pourrait faire l'objet de sanctions.

Tout membre du personnel est personnellement responsable du contenu qu'il publie sur les espaces publics en ligne.

CHAPITRE V. PROTECTION DES ORDINATEURS ET INFORMATIONS

Article 18.

Le membre du personnel contribue à la sécurité du système d'information notamment en respectant les principes suivants:

Intégrité	a) vérifier l'origine et le caractère inoffensif des sites Web visités et des messages entrants ; b) éviter autant que possible l'ouverture de spams et annexes non fiables, ainsi que le téléchargement de fichiers non fiables ; c) éviter de cliquer sur des liens contenus dans de tels e-mails, sites Web et fichiers non fiables ; d) signaler les courriers indésirables en fonction des moyens mis à votre disposition (https://intranet.bruxelles.be/alerte-e-mail-securite-mot-de-passe) ;
Mots de passe et sécurité	e) choisir un mot de passe qui n'est pas facile à deviner, et le modifier régulièrement tout en s'assurant qu'il soit conforme à la politique des mots de passe f) utiliser la double authentification (MFA) en fonction des moyens mis à sa disposition
Accès au poste de travail	g) verrouiller son ordinateur et les autres appareils en quittant son poste de travail ;
Stockage	h) d'utiliser les emplacements sur le réseau pour le stockage de fichiers professionnels, et non le disque dur, sauf s'il s'agit de documents préparatoires ; i) de prendre conscience du fait que le disque local ne fait l'objet d'aucune sauvegarde.

Article 19.

Aucun membre du personnel ne peut:

Mots de passe	a) partager son mot de passe avec d'autres personnes, qu'il s'agisse de membres du personnel de la Ville ou d'externes (prestataire de services ICT, consultants, amis, membres de la famille...) ; b) demander, recevoir ou utiliser le mot de passe d'un collègue ; c) prendre note sur un support physique ou numérique d'un mot de passe ; d) utiliser le même mot de passe pour des comptes privés et professionnels ;
Accès aux comptes	e) donner accès à son compte à d'autres personnes, qu'elles soient internes ou externes ; f) demander, recevoir ou utiliser l'accès au compte d'un collègue ;
Abus, sabotageou vandalisme	g) faire un usage impropre de vulnérabilités découvertes dans le système ; h) endommager du matériel, des logiciels, des fichiers ou des processus, internes ou externes, ou les modifier ou supprimer de manière illicite ; i) consulter des données soumises à droit d'autrui ou des données à caractère personnel qui ne sont pas nécessaires à la fonction. j) dissimuler le fait de pouvoir accéder à des données normalement inaccessibles
Logiciel	k) installer ou utiliser des logiciels non autorisés, c'est-à-dire des logiciels n'ayant pas obtenu l'autorisation écrite préalable d'un supérieur hiérarchique, ou des logiciels n'étant pas destinés à l'exercice d'activités professionnelles (exemple : outil gratuit en ligne); l) lancer en connaissance de cause des fichiers exécutables (par ex. « .exe »»), sauf moyennant l'accord du prestataire de services ICT

Matériel	m) connecter des supports amovibles (clés USB, smartphones, disque externe...), sauf si leur origine et leur contenu sont connus ; n) connecter du matériel non fourni par i-City, à l'exception de périphériques ne nécessitant pas d'installation logicielle avec droits d'administrateur (clavier, souris, écran, oreillette bluetooth, ...) et pour lesquels aucun support n'est dû par i-City ;
Stockage	o) sauvegarder des fichiers liés au travail sur des services de cloud qui ne sont pas fournis par la Ville (Dropbox...) ; p) stocker des données liées au travail à une adresse privée ; q) supprimer des fichiers sur des dossiers partagés sans approbation explicite du propriétaire du document (+ mention du motif pour lequel le document doit être supprimé) ;
Travail à distance	r) laisser son PC ou d'autres appareils mobiles sans surveillance et/ou déverrouillés, en particulier à un endroit où ils pourraient faire l'objet d'un vol ; s) se rendre dans des espaces publics avec des informations soumises à droit d'autrui (par ex. où elles peuvent être lues) ; t) emporter à son domicile des pages imprimées comportant des informations soumises à droit d'autrui, car elles sont difficiles à protéger.

CHAPITRE VI. RESPONSABILITÉ DU MEMBRE DU PERSONNEL

Article 20.

En cas de non-respect des dispositions de la présente politique, le membre du personnel pourra être tenu pour responsable selon les règles en matière de responsabilité civile du membre du personnel (dol, faute lourde ou faute légère répétitive).

En dehors de la responsabilité civile, le non-respect des dispositions de la présente convention pourra faire l'objet de sanctions disciplinaires.

À titre d'exemple et de manière non-exhaustive, pendant et en dehors des heures de travail, pourraient s'apparenter à un motif grave :

- toute rupture volontaire de l'obligation de confidentialité (ex. : diffusion de données soumises à droit d'autrui ou à caractère personnel, accès non autorisé à du contenu professionnel)
- toute entrave au code de déontologie, notamment la publication de propos haineux, calomnieux ou répréhensibles sur les espaces publics en ligne. Seront considérées comme contraire au code de déontologie, les publications :
    - de nature pornographique répréhensible, tel que la pédopornographie ou des captures d'agressions sexuelles…
    - racistes ou haineuses envers les étrangers ;
    - discriminant sur la base du sexe, de l'orientation sexuelle, du handicap, de la croyance, de convictions philosophiques ou politiques ;
    - révisionnistes ;
    - qui contiennent ou favorisent un comportement de harcèlement moral ou sexuel ;
    - qui sont contraires aux bonnes mœurs

- Tout comportement portant délibérément atteinte à la sécurité du système d'information (ex : piratage).

La présente disposition n'entre pas en contradiction avec l'éventuelle responsabilité pénale du membre du personnel en cas d'utilisation répréhensible des moyens ICT.

Article 21.

En cas de comportement risqué pour la sécurité du système d'information, l'employeur se réserve le droit de révoquer avec prise d'effet immédiat l'accès du membre du personnel à son compte.

Article 22.

Le membre du personnel est réputé avoir pris connaissance de l'intégralité de la présente politique et la respecter.

Le membre du personnel est invité par son supérieur hiérarchique, ou lors de son recrutement, à signer une prise de connaissance.

Article 23.

La présente politique doit toujours être interprétée et appliquée en vue du bon fonctionnement des services de la Ville, et de la sécurité et du bon usage des moyens ICT et des réseaux de la Ville.

Si le membre du personnel, après avoir parcouru la présente politique, n'est pas sûr de ce qu'il faut entendre par un usage acceptable des moyens ICT, de ce qu'il peut faire ou non ou des mesures de sécurité qu'il doit prendre pour préserver l'intégrité du système informatique, il est tenu de demander un encadrement et des clarifications auprès de sa direction ou son correspondant informatique (adjoint).

Article 24.

Le membre du personnel est tenu, s'il constate un incident informatique affectant la sécurité des informations et des ordinateurs dans le cadre de la présente politique, d'en faire immédiatement mention au CISO (via security@brucity.be), pour éviter tout nouveau dommage ou incident, que cela le concerne lui, ou concerne ses collaborateurs et son environnement de travail. Le membre du personnel est invité à ne rien entreprendre de plus à ce moment tant qu'il n'aura pas été autorisé à le faire.

Article 25.

Le membre du personnel est tenu s'il constate un incident de données à caractère personnel (perte de confidentialité, d'intégrité, ou de disponibilité de données à caractère personnel) d'en informer immédiatement le DPO à l'adresse privacy@brucity.be

Article 26.

Toute violation des dispositions de la présente politique peut donner lieu à des procédures et sanctions disciplinaires.

CHAPITRE VII. RESPECT DE LA VIE PRIVÉE DU MEMBRE DU PERSONNEL

Section 1 - PROTECTION DES DONNÉES DU MEMBRE DU PERSONNEL

Article 27.

Les traitements de données qui concernent le membre du personnel sont décrits dans la Charte vie privée relative à la protection des données des membres du personnel de la ville de Bruxelles, disponible sur l'intranet. La Ville traite les données de son personnel en conformité avec leur droit à la vie privée, en ce compris le RGPD et/ou la loi vie privée.

La Ville attache une grande importance au respect de la vie privée de ses membres du personnel et respecte de près la loi sur la vie privée. Lorsqu'elle décide de procéder à un contrôle, elle s'engage à le faire en conformité avec les principes de finalité, de proportionnalité et de transparence prescrits par cette loi (voir chapitre VIII).

Section 2 - PROCÉDURE EN CAS DE CONTRÔLE DE L'UTILISATION DES MOYENS ICT PAR LE MEMBRE DU PERSONNEL

Article 28. Contrôle global.

La ville peut organiser une surveillance systématique et globale de l'utilisation d'une application professionnelle. Toutefois, cette surveillance devra impérativement respecter les principes de la CCT 81 et les recommandations en termes de respect de la Vie privée.

Tout contrôle systématique de l'utilisation des moyens ICT ou applications mises à disposition du personnel doit obligatoirement faire l'objet d'un règlement spécifique, validé par une procédure concertée incluant le DPO. Ce règlement doit notamment contenir les mesures de protection suivantes :

A) Principe de finalité

Le contrôle sur l'utilisation des moyens ICT peut uniquement avoir lieu si une ou plusieurs des finalités suivantes sont visées :

- la sécurité et/ou le bon fonctionnement des systèmes informatiques, ainsi que la protection physique du matériel ;
- la prévention de faits illicites ou contraires aux bonnes mœurs, ou qui nuisent à la dignitéd'autrui ;
- le respect de manière honorable des directives d'utilisation concernant les moyens ICT telles que mentionnées dans le présent document ;
- la protection de la réputation et des intérêts sociaux et économiques de la Ville et de ses institutions ;
- la protection de la vie privée, de la dignité et de la réputation de ses membres du personnel
- la protection de la vie privée des citoyens ;

B) Principe de transparence : information préalable, collective ou individuelle, des membres du personnel. Cette information spécifie les modalités, la finalité et la durée du contrôle ainsi que les éventuelles sanctions.

C) Principe de proportionnalité : le contrôle ne peut prendre la forme d'une ingérence systématique et sans fin, mais doit se limiter à la durée nécessaire pour accomplir la finalité poursuivie.

D) Principe d'individualisation en cascade

La Ville se réserve le droit, dans le cadre des finalités et de la procédure décrites ci-avant, de procéder à l'identification du membre du personnel concerné. Ce contrôle peut uniquement donner lieu à l'identification d'un membre du personnel si elle a pour but :

- de prévenir des faits illicites ou contraires aux bonnes mœurs, ou qui nuisent à la dignitéd'autrui ;
- de protéger les intérêts économiques et financiers de la Ville ;
- d'assurer la sécurité ou le fonctionnement des systèmes informatiques ;
- de mettre un terme à toute autre infraction aux prescriptions de sécurité.

Dans les autres cas, comme une violation du respect des règles d'utilisation des moyens ICT, une identification ne peut avoir lieu que lorsque le personnel a d'abord été collectivement averti de la violation de ces règles et si une violation similaire a à nouveau eu lieu.

Article 29. Contrôle exceptionnel

Lorsqu'un abus répété ou un usage interdit, c'est-à-dire une infraction aux mesures de sécurité et directives d'utilisation énumérées dans la présente politique, est présumé notamment par un faisceau de preuves découvertes fortuitement, le chef de département, ci-après dénommé le demandeur du contrôle, peut en informer le DPO. Il mentionne alors de manière explicite et écrite l'abus répété ou l'usage interdit suspecté.

Le DPO rend un avis indépendant sur la légitimité, la proportionnalité, la nécessité et la légalité du contrôle. Cet avis indique les mesures de protection de la vie privée à respecter dans le cadre du contrôle. Seul le Secrétaire Communal peut décider de poursuivre l'enquête et de surveiller l'utilisation des moyens ICT.

L'enquête ne peut viser que la recherche de la preuve des faits reprochés et ne peut en aucun cas découler sur un contrôle plus élargi que le contrôle initialement demandé.

La Ville ne permet des contrôles que dans le cadre des principes décrits dans cette politique, ne fait en aucun cas un usage permanent de ces capacités, et ne procède à aucun contrôle permanent et systématique du membre du personnel.

Le membre du personnel concerné par un contrôle sera notifié de ce contrôle préalablement à sa mise en œuvre.

Le contrôle décrit ci-dessus ne concerne pas l'irrespect des dispositions qualifiées en tant que recommandations et bonnes pratiques dans la présente politique.

Article 30.

Le responsable de l'exécution de ce contrôle est le prestataire de services ICT. Ce dernier a notamment la capacité technique de :

- créer une liste générale de tous les sites Web visités par le biais de son réseau, avec mention de la durée de la visite et du moment auquel elle est intervenue ;
- surveiller à propos du trafic d'e-mails des éléments comme la fréquence, le nombre, la taille, les annexes... ;
- consulter les données de communication par téléphone ou fax telles qu'elles ont été facturées ;

Le prestataire de services ICT assurera un traitement confidentiel des données et elles pourront être conservées pendant la durée de l'enquête ou le temps nécessaire au déroulement d'une procédure judiciaire.

Lorsque le prestataire de services ICT constate une déviation, il en informe le DPO. On entend par déviation toute infraction aux directives de la présente politique. Les

déviations sont formellement établies par le demandeur du contrôle, qui établit un rapport écrit.

Article 31.

La Ville se réserve le droit, dans le cadre des finalités et procédures décrites ci-dessous, de procéder à l'identification du membre du personnel concerné. Ce contrôle peut uniquement aboutir à l'identification directe d'un membre du personnel s'il a pour but:

- de prévenir des faits illégaux ou contraires aux bonnes mœurs ou qui attenteraient à l'honneur des personnes ;
- de protéger les intérêts économiques et financiers de la Ville ;
- d'assurer la sécurité du fonctionnement des systèmes informatiques ;
- mettre un terme à toute autre infraction aux consignes de sécurité ;

Dans les autres cas, comme par ex. s'il s'agit d'une infraction à l'observation de règles d'usage des moyens ICT, l'identification ne pourra être réalisée qu'après que le personnel ait été collectivement prévenu que ces règles ont été non respectées et quand des infractions similaires ont à nouveau été observées.

Article 32.

Le membre du personnel concerné a le droit:

- de recevoir toutes les informations relatives auprès du DPO (**droit d'accès et droit à l'information**) ;
- de demander au DPO de détruire ou rectifier ces informations si elles s'avèrent incorrectes ou en violation avec la réglementation reprise dans la présente politique ou remontent à il y a plus d'un an (**droit de rectification et droit d'effacement des données**) ;
- de s'opposer, jusqu'à un mois après avoir été informé du contrôle, à ce dernier auprès duSecrétaire Communal (**droit d'opposition**) ou de demander la suspension du contrôle dans la mesure où il est contraire à la législation en vigueur (**droit de limitation**).
- de contester toute décision automatisée dans le cadre du contrôle et d'exiger l'intervention humaine dans la décision (**droit de ne pas faire l'objet d'une décision automatisée).**
- d'obtenir, par exception à l'article 20§3 du RGPD, les données du contrôle liées à la relation de travail dans un format structuré, couramment utilisé et lisible par machine et le droit de communiquer ces données à un autre responsable sans que la Ville ne s'y oppose (**droit à la portabilité**).

Toutes ces demandes peuvent être adressées au DPO.

CHAPITRE VIII. CONTRÔLE DE LA QUALITÉ

Article 33.

Une évaluation de la présente politique sera réalisée régulièrement, afin de revoir les directives susmentionnées en fonction :

- de nouveaux moyens de communication et technologies utilisés par les membres dupersonnel de la Ville;
- d'une évolution du cadre légal ;
- du contrôle de l'élaboration et de l'efficacité des procédures de contrôle ;

- de toute autre raison réputée nécessaire par l’employeur ou d’autres parties prenantes.