POLITIQUE ICT

Directives concernant les moyens ICT

Dernière modification: xx.xx.2020~~23.04.2018~~

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 la propriété de la Ville ou ont trait à la vie privée des membres du personnel ou de citoyens, et de garantir leur vie privée, conformément à la loi sur la vie privée.

Les membres du personnel ont généralement une adresse e-mail propre, accès à Internet, à la téléphonie et à la communication électronique, depuis leur poste de travail fixe ou éventuellement 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.- 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, membres 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 téléphones fixes 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 confidentielles	Les données confidentielles sont des données qui, en fonction de la situation, - sont uniquement destinées à un usage interne, - peuvent uniquement être consultées par quelques personnes habilitées, - ou qui sont protégées par la loi sur la vie privée.
Loi sur la vie privée	La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.
Le fichier	Ensemble de données (informatiques) ordonnées, comme un document de traitement de texte, des dépliants, des illustrations...
Réseaux sociaux	Toute forme de communication publique sur l'Internet. Quelques exemples de réseaux sociaux (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 messages courts (Twitter…), sites Web de publication de contenu (Wikipédia…)…
Chief Information Security Officer (CISO)	La personne qui détermine s'il est procédé ou non à un contrôle et à qui les incidents informatiques doivent être notifiés. Voir chapitre 7. Joignable via security@gial.be
Prestataire de services ICT	Celui qui met à disposition les moyens ICT ou les exploitent dans le cadre d'une relation contractuelle avec la Ville.

CHAPITRE II.
MATÉRIEL.

Article 2.- Plusieurs moyens ICT standard sont mis à la disposition de chaque membre du personnel de la Ville en fonction de leur position. Ces moyens restent la propriété de l'employeur. Le membre du personnel a l'obligation de prendre soin de ces moyens.

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 cas de leur 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 et de remettre le procès-verbal à la direction Développements et Organisation.

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 bon père de famille.

CHAPITRE III.
UTILISATION DES MOYENS ICT

Article 4.- Toutes les directives suivantes concernant l'utilisation s'appliquent à tous ces moyens, 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.

Section I.- Usage professionnel.

Article 5.- Pour les directives concernant un usage professionnel des moyens ICT, la direction peut imposer des exigences plus strictes ; le membre du personnel est de toute manière tenu

Correspondance	a) d'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) de régulièrement consulter son courrier entrant, d'y répondre à temps et

	d'éventuellement indiquer le délai dans lequel une suite pourra être donnée au message ; c) de limiter le nombre de destinataires dans les e-mails au nécessaire absolu ; d) de ne qualifier un message d'urgent que si c'est vraiment nécessaire ; e) en cas d'envoi erroné d'un e-mail, de 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, de ne pas l'ouvrir et le supprimer directement ;
Signature et police de caractères	g) d'utiliser la signature d'e-mail standardisée et la police de caractères standardisée - elles sont fixées par la cellule Communication et sont disponibles dans la charte graphique ;
Out of office	h) en cas d'absence de plus d'un jour, de rédiger un message d'absence de bureau (en cas de maladie, le faire par le biais du webmail[1]) - 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) d'éviter de joindre des fichiers volumineux en annexe à des e-mails ; j) de faire référence à un dossier partagé au lieu de joindre des fichiers à des e-mails ;
Imprimer	k) d'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 ;
Archiver	l) de régulièrement nettoyer sa messagerie et de n'y conserver que les messages pouvant encore servir ou ne pouvant être supprimés ; m) d'archiver sa messagerie avant de supprimer des messages et fichiers ;
Calendrier	n) d'indiquer dans son calendrier Outlook toutes ses indisponibilités en établissant une distinction entre indisponibilité pour occupation et indisponibilité pour absence ;
Durabilité	o) d'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 6.- 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 du personnel ne peut en aucun cas le modifier.

Article 7.- 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

1 Par ex. webmail.brucity.be

	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 II.- Usage privé.

Article 8.- Un usage privé raisonnable des moyens ICT est autorisé s'il

a) est non fréquent et de courte durée ;
b) n'a pas d'impact sur les obligations du membre du personnel ou ses collaborateurs ;
c) n'a pas d'impact sur le fonctionnement de la Ville ;
d) n'induit aucuns frais supplémentaires pour la Ville ;
e) ne contrevient pas aux autres parties de la présente politique ;
f) ne contrevient pas 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 privés de manière exhaustive ; copier ou imprimer un livre ; téléphoner à l'étranger ; faire des recherches personnelles dans des applications professionnelles.

Article 9.- L'usage privé de l'adresse e-mail professionnelle est autorisé lorsque le membre du personnel qualifie les e-mails sortants de personnels[2] 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.

Article 10.- 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 supprimer ces données.

Section III.- Usage non autorisé

Article 11.- Aucun membre du personnel ne peut

Contenu inadapté	a) visiter des sites Web, envoyer ou répondre à des messages dont le contenu i. est de nature érotique ou pornographique ; ii. est raciste ou haineux envers les étrangers ;

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

	iii. est discriminant sur la base du sexe, de l'orientation sexuelle, du handicap, de la croyance, de convictions philosophiques ou politiques ; iv. est révisionniste ; v. contient ou favorise un comportement de harcèlement moral ou sexuel ; vi. est irrespectueux vis-à-vis d'autrui ; vii. ou est de toute autre manière contraire aux bonnes mœurs, ou nuit à la dignité d'autrui ;
Usage illégal	b) 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 confidentielles	c) diffuser des données confidentielles concernant la Ville, ses établissements, membres du personnel, services, partenaires commerciaux, clients ou autres intéressés, sauf dans le cadre de ses obligations ; d) partager du contenu protégé par la loi sur la vie privée ;
Usage frivole	e) diffuser des chaînes de lettres, jouer à des jeux, passer du temps dans des chatrooms en ligne et autres ; f) écouter longtemps et en streaming de la musique et/ou des vidéos qui ne s'inscrivent pas dans le cadre du travail ; g) télécharger des fichiers volumineux ;
Usage commercial	h) s'engager dans des activités personnelles à but commercial ou faire de la publicité d'intérêts étrangers à ceux de la Ville ;
Calomnie	i) calomnier la Ville, ses établissements, services, membres du personnel, partenaires commerciaux, clients ou autres intéressés ;
Diffusion de l'opinion proper	j) utiliser la signature officielle dans des correspondances privées ; k) faire passer des opinions propres pour des opinions officielles de la Ville, ou parler de manière non autorisée en son nom.

Article 12.- 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 susmentionnées.

Section IV.- Concernant les réseaux sociaux

Article 13.- Cette partie de la politique a trait à l'usage personnel des réseaux sociaux, et principalement la **publication** d'avis, de commentaires, de photos, de rapports de statut ou d'autres contenus, dans les limites de l'article 8 relatif à l'usage privé.

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 ne disposant pas d'une telle autorisation ne peuvent s'adonner sur les réseaux sociaux à des activités 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 14.- Toutes les directives de la présente politique concernant l'utilisation de moyens ICT s'appliquent également à l'utilisation des réseaux sociaux sur le lieu de travail ou en déplacement dans le cadre du travail ou du télétravail.

En marge de ces directives, il est à tout moment interdit au collaborateur, lorsqu'il se rend sur les réseaux sociaux, même à partir de moyens ICT personnels et en dehors des heures de travail,

Données confidentielles	a) de diffuser des données confidentielles concernant la Ville, ses établissements, membres du personnel, services, partenaires commerciaux, clients ou autres intéressés ;
Calomnie	b) de calomnier la Ville, ses établissements, membres du personnel, services, partenaires commerciaux et autres intéressés ;
Données inexactes	c) de formuler des déclarations mensongères, trompeuses ou source de confusion concernant la Ville, ses établissements, membres du personnel, services, partenaires commerciaux et autres intéressés ; d) de se prononcer pour une autre personne qui est liée à la Ville; e) de publier des informations erronées concernant son expérience ou ses responsabilités professionnelles au sein de la Ville;
Activités du personnel	f) de publier des photos ou vidéos d'activités du personnel sans consentement explicite des personnes représentées.

Article 15.- Vu qu'il est pratiquement impossible d'effacer un message qui a été envoyé par l'Internet, le membre du personnel est invité à bien réfléchir avant de communiquer par le biais des réseaux sociaux ou de partager du contenu d'autres personnes par le biais des réseaux sociaux, afin de ne commettre aucune infraction aux directives de la présente politique.

Le membre du personnel doit également 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.

Tout membre du personnel est personnellement responsable du contenu qu'il publie sur les réseaux sociaux.

Article 16.- L'employeur se réserve le droit de consulter les activités du membre du personnel sur les réseaux sociaux si elles ont trait à la Ville et, le cas échéant, d'y donner suite si une infraction aux règles susmentionnées relatives à l'utilisation des réseaux sociaux est constatée.

CHAPITRE IV.

PROTECTION DES ORDINATEURS ET INFORMATIONS

Article 17.- Le membre du personnel est tenu

Intégrité	a) de vérifier l'origine et le caractère inoffensif des sites Web visités et des messages entrants ; b) d'éviter autant que possible l'ouverture de spams et annexes non fiables, ainsi que le téléchargement de fichiers non fiables ;

	c) d'éviter de cliquer sur des liens contenus dans de tels e-mails, sites Web et fichiers non fiables ;
Mots de passe et sécurité	d) de choisir un mot de passe qui n'est pas facile à deviner, et de le modifier régulièrement tout en s'assurant qu'il soit conforme à la politique des mots de passe ;
Accès au poste de travail	e) de verrouiller son ordinateur et les autres appareils en quittant son poste de travail ;
Stockage	f) 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 ; g) de prendre conscience du fait que le disque local ne fait l'objet d'aucune sauvegarde.

Article 18.- 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, sabotage ou 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 ;
Logiciel	i) 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 ; j) lancer en connaissance de cause des fichiers exécutables (par ex. « .exe »), sauf moyennant l'accord du prestataire de services ICT ;
Matériel	k) ~~connecter des supports amovibles, sauf si leur origine et leur contenu sont connus~~ connecter des supports amovibles (clés USB, smartphones, disque externe...), sauf si leur origine et leur contenu sont connus ; l) ~~connecter du matériel propre (clés USB, smartphones...) à l'ordinateur, sauf s'il a fait l'objet d'un scanner antivirus~~ connecter du matériel non fourni par i-City, à l'exception de périphériques ne nécessitant pas d'installation logicielles avec droits d'administrateur (clavier, souris, écran, oreillette bluetooth, ...) et pour lesquels aucun support n'est dû par i-City ;

Stockage	m) sauvegarder des fichiers liés au travail sur des services de cloud qui ne sont pas directement liés à la profession (Dropbox...) ; n) transmettre des données liées au travail à une adresse privée ; o) 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	p) 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 ; q) se rendre dans des espaces publics avec des informations confidentielles (par ex. où elles peuvent être lues) ; r) emporter à son domicile des pages imprimées comportant des informations confidentielles, car elles sont difficiles à protéger.

Article 19.- En cas de non-respect des directives susmentionnées, le membre du personnel sera dans tous les cas tenu pour responsable de tout usage de son compte, par lui-même ou autrui.

Article 20.- L'employeur se réserve le droit de révoquer avec prise d'effet immédiate l'accès du membre du personnel à son compte.

CHAPITRE V.
RESPONSABILITÉ DU MEMBRE DU PERSONNEL

Article 21.- 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 22.- 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 23.- 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@gial.be), pour éviter tout nouveau dommage ou incident. Et ce 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 24.- Toute violation des directives de la présente politique peut donner lieu à des procédures et sanctions disciplinaires selon le statut.

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

Article 25.- 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 plus haut la partie consacrée à l'usage privé).

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 7).

Note : les procédures suivantes seront revues dans le cadre de l'application des directives du Règlement général sur la protection des données qui entrera en vigueur le 25 mai 2018.

CHAPITRE VII.
SURVEILLANCE

Article 26.- Lorsqu'un abus 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, le chef de département, ci-après dénommé le demandeur du contrôle, peut en informer le CISO de manière confidentielle. Il mentionne alors de manière explicite et écrite l'abus ou l'usage interdit suspecté.

Seul le CISO peut décider de poursuivre l'enquête et de surveiller l'utilisation des moyens ICT.

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

Les infractions décelées lors de la surveillance menée dans le cadre d'un but supérieur peuvent donner lieu aux procédures suivantes.

Article 27.-

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 dignité d'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 et partenaires commerciaux ;
- la protection de la vie privée des citoyens ;

Principe de proportionnalité

Lorsqu'une décision de procéder à un contrôle est prise, il ne peut prendre la forme d'une ingérence systématique et sans fin, mais doit se limiter à un minimum et ne peut avoir lieu qu'à titre complémentaire si le demandeur du contrôle l'estime nécessaire par le biais d'un rapport écrit.

Principe de transparence

Les procédures de contrôle sont communiquées à l'ensemble du personnel de la Ville par le biais de la présente politique.

Article 28.- 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 ;
- de surveiller à propos du trafic d'e-mails des éléments comme la fréquence, le nombre, la taille, les annexes... ;
- de 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 CISO. 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 29.- La Ville se réserve le droit, dans le cadre des finalités 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 dignité d'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 30.- Le membre du personnel a le droit

- de demander jusqu'à un mois après avoir été informé du contrôle toutes les informations relatives à ce dernier auprès du CISO (droit de regard) ;
- de demander au CISO de détruire 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 de suppression des données) ;

- de s'opposer, jusqu'à un mois après avoir été informé du contrôle, à ce dernier auprès du Secrétaire Communale (droit d'opposition).

CHAPITRE VIII.
CONTRÔLE DE LA QUALITÉ

Article 31.- Une évaluation de la présente politique sera réalisée régulièrement, une fois par an au maximum, afin de revoir les directives susmentionnées en fonction

- de nouveaux moyens de communication et technologies utilisés par les membres du personnel 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.