Charte des utilisateurs du système d'information de la Ville de Paris

Version du comité social territorial central du 24 novembre 2025

Table des matières

I. Les enjeux de la charte informatique

La présente Charte définit les règles d'accès et d'usage des ressources informatiques de la Ville de Paris et de ses établissements publics partageant le même système d'information (le Centre d'Action Sociale de la Ville de Paris, l'Établissement Public Paris Musées, l'Ecole du Breuil...). Dans la suite du document, l'ensemble de ces administrations est désigné par le vocable : "La Ville de Paris".

L'ensemble des personnels habilités à exercer une fonction technique sur le système informatique est désigné par le vocable « Service Informatique ».

L'ensemble des directives et des recommandations de la Charte définit le cadre normatif destiné à protéger les ressources informatiques, les systèmes d'information, et à offrir un service performant et sécurisé à l'ensemble des utilisateurs. Si la présente charte ne peut couvrir de façon exhaustive tous les cas de figures possibles, elle fixe les principes généraux d'utilisation du système d'information permettant de protéger les ressources de la Ville de Paris dans le respect de la réglementation en vigueur.

Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires qui s'imposent.

Le « bon usage » des ressources informatiques et des systèmes d'information est un usage responsable : il fait appel au bon sens, à l'attention et à la prudence, il s'appuie sur des recommandations techniques ou d'usage, mais il se réfère également à des règles de déontologie professionnelle, de déontologie personnelle et à des bonnes pratiques de numérique responsable.

La sécurité et le bon fonctionnement du Système d'Information sont l'affaire de tous et découlent d'une action à la fois collective et individuelle. Chacun doit être conscient de sa responsabilité dans la sécurité globale du système d'information de la Ville de Paris. La sécurité des systèmes d'information est un objectif partagé qui ne peut être atteint que dans un climat de loyauté et de confiance réciproque.

Une première version de la charte a été publiée en Octobre 2014. Les évolutions techniques et d'usage nécessitent la présente mise à jour.

Le champ d'application de la Charte

La présente Charte s'applique à l'ensemble des utilisateurs du système d'information (SI) de la Ville de Paris, donc y compris au personnel des entités sous-traitantes et des partenaires externes accédant au SI de la Ville de Paris.

Les entités chargées des relations contractuelles et opérationnelles avec ces sous-traitants, ou partenaires, doivent, en conséquence, s'assurer du respect de la Charte sur le périmètre d'actions impactant le SI.

Le système d'information est considéré dans son ensemble, c'est-à-dire comme la totalité des moyens informatiques ou de télécommunications (postes de travail, dont les ordinateurs, réseaux, internet, téléphones, tablettes…) et des données visant à créer, acquérir, traiter stocker, archiver, diffuser ou détruire de l'information en rapport avec l'activité professionnelle des utilisateurs du SI.

Les règles édictées dans ce document s'appliquent également à l'ensemble des équipements informatiques de la Ville de Paris ou qui interagissent avec le SI de l'institution. Il s'agit, à titre d'illustration, des équipements fournis par la Ville de Paris ou fournis par des partenaires et autorisés à être connectés au SI.

Les objectifs de la Charte

La présente Charte a pour objet de définir l'usage qui doit être fait par les utilisateurs du système d'information, dans le respect des droits, devoirs et obligations de chacun, en particulier ceux et celles qui s'appliquent à tout agent public de la Ville de Paris.

À ce titre, y sont rappelées les principales règles qui visent à :

- Maintenir la sécurité du SI et à ce titre : la confidentialité, l'intégrité, la disponibilité et la traçabilité du SI ;
- Maintenir à son meilleur niveau la qualité de service rendue par le SI dans le cadre de ses activités ;
- Promouvoir la sobriété numérique et à ce titre un usage du SI responsable qui tienne compte de son impact écologique ;
- Préciser la responsabilité des différents utilisateurs.

L'information des agents

Les utilisateurs sont informés individuellement du contenu de la présente Charte par un message lors de chaque connexion au système, rappelant son existence, l'endroit où elle est disponible ainsi que l'obligation de la consulter.

Cette charte est également remise avec le livret d'accueil et est disponible sur Intr@Paris.

Tout contrat passé entre la Ville de Paris et un tiers impliquant l'accès de ce tiers aux ressources informatiques et aux systèmes d'information de la Ville de Paris stipule que le contractant s'engage à faire respecter la présente Charte par son propre personnel et, le cas échéant, ses sous-traitants.

La Charte peut également être portée à la connaissance des personnes visées par tous moyens et notamment :

- par voie d'annexe au règlement intérieur de l'entité,
- par remise d'un exemplaire papier de la Charte.
- par voie d'affichage dans les locaux de l'entité,

La.le secrétaire général.e est chargé.e de l'exécution de la Charte au sein de la Ville de Paris. La DSIN met en place toutes les mesures techniques nécessaires à son application et au contrôle de son exécution.

Les directeurs (trices) et les délégué(e)s veillent au respect de la Charte au sein de l'entité dont ils sont responsables.

Les responsabilités réciproques du service informatique et des utilisateurs

Le service informatique est responsable du contrôle et du bon fonctionnement du système d'information et de communication.

Les membres du service informatique sont soumis au secret professionnel et ne doivent en aucun cas divulguer les informations qu'ils sont susceptibles de consulter ou de manipuler sauf en cas de menace pour la sécurité du SI, constatée par les responsables du Service Informatique, suivie d'une autorisation expresse de leur part.

Dans le cadre de la prise en main à distance d'un poste de travail par le support SI, l'autorisation préalable de l'utilisateur est obligatoire.

L'utilisateur est responsable quant à lui des ressources qui lui sont confiées dans le cadre de l'exercice de ses fonctions. Il doit concourir à la protection des dites ressources, en faisant preuve de prudence.

Par ailleurs, l'utilisateur ne doit pas nuire à l'intégrité du SI, à sa disponibilité ni à son fonctionnement normal.

L’utilisateur ne doit en aucun cas chercher à accéder, par des moyens détournés, à des informations ou des ressources, pour lesquelles il n’est pas habilité. Les actions qu’il effectue dans les applicatifs métier doivent être en adéquation avec ses missions.

L'utilisateur du SI est soumis à l’obligation de discrétion professionnelle et veille au respect de la confidentialité des informations en sa possession.

Il doit en toutes circonstances veiller au respect des droits de propriété intellectuelle, du secret des correspondances, de la confidentialité des données personnelles, de la protection des systèmes de traitement automatisé de données, et du droit à l'image des personnes.

Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer à une activité illicite ou portant atteinte aux intérêts de la Ville de Paris, y compris sur Internet.

Il est notamment interdit :

- De diffuser ou de télécharger des Informations protégées par le droit d’auteur qu'il s'agisse notamment d'écrits, d'images, de logiciels ou de bases de données, et de porter atteinte à tout signe distinctif appartenant à des tiers, en particulier aux droits de marques, nom commercial et nom de domaine ;
- De porter atteinte à la vie privée d’autrui (sujets relatifs entre autres aux opinions politiques, philosophiques ou religieuses, aux origines ethniques, à l’orientation sexuelle ou à la santé des personnes) ;
- De publier tout propos contraire à la loi (notamment la diffamation, l’injure, les incitations aux crimes, à la discrimination, à la haine notamment raciale, le révisionnisme et l’apologie des crimes, la compromission de mineurs ou leur exposition à des messages à caractère violent ou pornographique, ou toute incitation à la consommation de substances interdites), aux règles d’éthique et de déontologie, sur les réseaux sociaux en particulier ;
- De commettre tout acte relevant de la fraude informatique : falsification, modification, suppression ou introduction d'Informations avec l'intention de nuire ;
- De transmettre des informations professionnelles à des tiers sans y avoir été formellement autorisé.

La charte est ainsi conçue qu’elle permet à l’utilisateur du SI d’y trouver les directives et conseils rassemblés sous forme de fiches.

II. Les règles de bonne utilisation du système d'information

Fiche 1 : La bonne utilisation des ordinateurs

Sécurité physique

Les ordinateurs doivent être protégés physiquement, sur site ou en mobilité / télétravail.

Chacun doit veiller à utiliser les moyens de protection fournis par la Ville de Paris tels que les câbles antivols et les armoires à clé, afin d'éviter les vols ou la dégradation des équipements.

Cette mesure s'étend également au petit matériel : clefs ou périphériques USB notamment ou éventuels autres supports (DVD, CD...).

A l'occasion de ses déplacements professionnels ou de ses trajets domicile-travail, chacun doit conserver une constante surveillance sur ces différents matériels et les données qu'ils contiennent.

En cas de perte, vol d'un équipement ou suspicion de fuite d'informations, l'utilisateur doit informer immédiatement l'AIP au 01 42 76 89 89 et sa hiérarchie.

Mise en Veille

En cas d'absence, même temporaire, il est impératif que l'utilisateur verrouille l'accès au matériel qu'il utilise.

Afin d'empêcher tout risque d'intrusion dans le Système d'Information pouvant mener à des incidents de sécurité, telle que la fuite d'informations, chaque utilisateur doit s'assurer d'avoir verrouillé sa session, s'il est amené à laisser sa station de travail ou son équipement d'extrémité sans surveillance ou à quitter son bureau.

Arrêt des postes

Afin de limiter le temps d'exposition aux attaques (un poste allumé en permanence est plus longtemps exposé aux menaces) et afin de permettre aux installations nécessitant un redémarrage de se dérouler complétement, l'utilisateur veille à éteindre son poste régulièrement notamment la nuit et le weekend.

La DSIN met en œuvre une extinction automatique des postes fixes à 20h.

Configuration

Les postes de travail de la Ville de Paris doivent respecter les configurations établies par la DSIN (palier technique, réglages, installations, etc.).

Chaque utilisateur est responsable, sous le contrôle et la validation de sa hiérarchie, des ressources informatiques et de télécommunications mises à sa disposition ainsi que de l'utilisation qu'il en fait : il demeure, à cette occasion, soumis aux règles générales de discrétion professionnelle et de déontologie de la Ville de Paris.

Il ne doit pas modifier la configuration des postes ni entraver le fonctionnement des outils de sécurité tout particulièrement celui de :

- L'antivirus;
- L'EDR (Endpoint Detection and Response);
- Du pare-feu ;
- Des outils de distribution des correctifs de sécurité. L'application de ces correctifs est obligatoire ; □ De tout autre système de sécurité complémentaire.

L'utilisateur ne doit pas installer volontairement de logiciels, ni copier ou installer des fichiers susceptibles de créer des risques de sécurité au sein du SI de la Ville de Paris.

Il ne doit en aucun cas disposer d'outils permettant de contourner la sécurité notamment des logiciels de découverte de mot de passe, de prise à distance ou d'écoutes clandestines ou interception de trafic, de recherche et exploitation de vulnérabilités, décompilateur de programmes, logiciels pour générer des clefs de licence.

Certains postes manipulent des données sensibles (médicales, sociales ou confidentielles par exemples). Ces postes font l'objet de configurations spécifiques.

En aucun cas ces configurations ne doivent être modifiées d'une quelconque façon.

Si des prestataires utilisent des postes de travail non fournis par la Ville de Paris, ils s'engagent via le contrat qui les lient à la Ville, à veiller à la sécurité du matériel utilisé afin que celui-ci ne constitue pas un risque pour le SI.

Une attention particulière sera apportée à la lutte contre les programmes malveillants et au comblement des vulnérabilités afin que ces équipements ne constituent pas une source de risques pour le SI (intrusion, fuites de données, introduction de virus…A l'occasion de son départ de la collectivité, l'utilisateur a obligation de restituer tous les matériels informatiques de la Ville de Paris.

A défaut, la Ville de Paris peut émettre à son encontre un titre de recette correspondante à la valeur de l'équipement.

Fiche 2 : La bonne utilisation des smartphones et tablettes

Les équipements de type smartphones ou tablettes permettant de stocker et d'accéder à des Informations doivent être protégés.

Ils sont tout particulièrement exposés aux vols ou pertes.

L'utilisateur doit définir un code PIN et un code de déverrouillage. Le chiffrement des données est activé par le service informatique lorsque cela est techniquement possible.

L'utilisateur doit veiller aux permissions demandées par les applications et doit installer ces applications uniquement à partir des magasins ou sites de téléchargement officiels (« Stores »).

Aucune application identifiée comme susceptible de nuire à la sécurité du SI ne doit être installée sur ces équipements.

L'accès au SI à partir de smartphones ou de tablettes qui contourneraient les mécanismes de sécurité est strictement interdit (Manipulations de type « Jailbreaking » ou « rooting »).

A l'occasion de son départ de la collectivité, l'utilisateur a obligation de restituer tous les matériels informatiques de la Ville de Paris.

A défaut, la Ville de Paris peut émettre à son encontre un titre de recette correspondante à la valeur de l'équipement.

Fiche 3 : La bonne utilisation des imprimantes multifonctions (scanner-fax, copie, impressions)

L'envoi d'informations par télécopieur peut comporter des risques car l'identité de la personne qui réceptionnera le document peut difficilement être garantie. L'utilisation de ces appareils est donc déconseillée, dans la mesure du possible, pour des informations sensibles.

Les accusés d'envoi, contenant souvent une copie des éléments transmis, ne doivent pas être laissés sur les télécopieurs.

A l'impression, les documents confidentiels, contenant des informations personnelles ou des informations sensibles par exemple, doivent être récupérés immédiatement et ne pas rester sur l'imprimante.

Chaque fois que c'est possible il est recommandé de privilégier l'utilisation des imprimantes à mots de passe ou code de sécurité qui permettent de ne déclencher l'impression que lorsqu'on est en mesure de récupérer immédiatement les documents imprimés

Fiche 4 : La bonne utilisation des supports amovibles

Les supports amovibles (tels que les clés USB ou les disques externes) doivent être utilisés avec vigilance. Ils sont susceptibles d'héberger des programmes informatiques pouvant porter atteinte à l'intégrité du Système d'Information (par exemple des virus, des vers, ou des chevaux de Troie).

Il est demandé à chaque personne d'utiliser les matériels fournis par la Ville de Paris et de ne les connecter qu'à des postes de travail sécurisés (pourvus d'un antivirus, à jour de correctifs et respectant tous les standards de la Ville de Paris).

A l'occasion de son départ de la collectivité, l'utilisateur a obligation de restituer tous les matériels informatiques de la Ville de Paris.

A défaut, la Ville de Paris peut émettre à son encontre un titre de recette correspondante à la valeur de l'équipement.

Fiche 5 : La bonne utilisation du réseau

Accès depuis des locaux de la Ville de Paris

Depuis les locaux de la Ville de Paris, l'accès à Internet est uniquement autorisé à travers les infrastructures configurées et fournies par la Ville de Paris.

Afin de garantir l'intégrité du SI de la Ville de Paris, il est préconisé de privilégier le réseau wifi de la Ville de Paris quand il est accessible. Il est demandé à chaque utilisateur de ne jamais connecter de postes de travail simultanément au réseau de la Ville de Paris et à un réseau tiers car cette pratique augmente les risques d'intrusion.

Il est interdit d'installer tout équipement partageant une connexion réseau (Borne wifi par exemple).

Accès distants

Les accès distants au SI sont uniquement autorisés par le biais des systèmes de communication à distance mis en place par le Service Informatique. Ces moyens de communication (VPN, Monbureau ou dispositif équivalent mis en place par le service informatique...) permettent en particulier le télétravail des agents.

L'utilisateur ne cherchera pas à accéder à distance aux ressources informatiques par d'autres moyens.

L'utilisateur veillera à garantir la sécurité du terminal d'accès utilisé et il protégera les données qui pourraient être stockées localement de manière temporaire.

Télétravail

L'agent en télétravail veillera à ce qu'il reste la seule personne à utiliser le poste professionnel : aucune personne de son entourage n'est autorisée à utiliser le matériel mis à disposition par la Ville.

Il doit être particulièrement vigilant pour protéger le portable utilisé dans les transports et les lieux publics (vols, pertes, chocs, indiscrétions et espionnages).

Fiche 6 : La bonne utilisation des comptes utilisateurs

Les comptes d'accès au SI sont strictement personnels et confidentiels.

Les droits d'accès à tout ou partie du SI reposent sur un compte d'accès strictement personnel composé d'un identifiant et d'un mot de passe.

En matière de protection et de gestion des mots de passe l'utilisateur respecte les consignes édictées par le Service informatique (complexité, fréquence de changement, etc.)

Les moyens d'authentification sont strictement confidentiels et ne doivent en aucun cas être communiqués à une tierce personne y compris au support SI (AIP), dans le cadre de leurs interventions. La divulgation volontaire ou par négligence de codes d'accès est considérée comme une faute professionnelle et susceptible de sanctions.

Si un utilisateur a communiqué son identifiant et son mot de passe ou s'il soupçonne une compromission ou une utilisation anormale de son compte, il veille à changer immédiatement son mot de passe.

L'utilisateur est seul responsable des actions réalisées depuis son compte d'accès.

En aucun cas le Service Informatique n'est habilité à communiquer le mot de passe d'un utilisateur à un tiers.

Les mots de passe fournis par défaut par les éditeurs ou les fabricants seront remplacés immédiatement lors de l'installation ou la mise à jour d'un système.

Si un compte ou une ressource n'est pas directement rattaché à une personne physique, (messagerie fonctionnelle de service ou compte applicatif par exemple) une personne doit être dûment désignée comme responsable de l'utilisation faite de cette ressource.

Fiche 7 : La bonne utilisation des espaces de stockage des données

La Ville de Paris met à la disposition des utilisateurs des répertoires et des outils collaboratifs permettant de sauvegarder et partager des informations.

Les informations professionnelles nécessaires à la continuité des activités doivent être stockées sur les répertoires réseaux du SI ou dans les applications dédiées à ces activités.

L'utilisateur ne doit conserver que le minimum d'informations en local sur son ordinateur professionnel et doit veiller à transférer les informations stockées en local sur les répertoires réseaux du SI de façon à ce que ces données soient sauvegardées.

L'utilisateur est responsable des informations et doit veiller à préserver la confidentialité des informations et à ne les partager qu'avec les personnes habilitées à y accéder.

Il doit être particulièrement vigilant avec les données sensibles ou confidentielles.

Les services d'hébergement externalisés fournis par des tiers (offre Cloud) peuvent comporter des failles pouvant constituer une menace pour la sécurité du Système d'Information et des Informations stockées. Seuls les services Cloud mis à disposition ou autorisés par le service informatique peuvent être utilisés pour le stockage ou traitement d'informations professionnelles.

L'utilisateur ne doit pas effacer, supprimer ou modifier, de sa propre initiative, des informations pouvant être nécessaires au bon déroulement des activités et des services rendus par la Ville de Paris.

Fiche 8 : La bonne utilisation des applications

Les services de la ville utilisent au quotidien les outils numériques dans le cadre de leurs missions et de leurs métiers.

Ils s'appuient sur des services numériques ou des outils bureautiques mis à disposition par le service informatique.

Il est interdit à un service de mener une activité métier sur une application développée par ses soins ou achetée à un tiers dont l'acquisition ou le développement n'a pas été autorisé préalablement par le service informatique. Cet accord doit être obtenu par note administrative.

Le Service informatique ne saurait être tenu pour responsable du bon fonctionnement d'un outil qu'il n'a pas acquis ou conçu. Il n'a aucune obligation à reprendre les données d'exploitation et de maintenance d'un outil acquis ou développé sans son accord.

Fiche 9 : La bonne utilisation d'internet

Utilisation

Dans le cadre de ses missions, un utilisateur peut avoir accès à Internet.

La consultation de sites Internet ou le téléchargement de fichiers qui pourraient, au sens le plus large, être considérés comme illégaux sont interdits.

Pour des raisons de sécurité ou sur décision de la Ville de Paris, l'accès à certains sites peut être limité ou prohibé par le Service Informatique.

Celui-ci est habilité à imposer des configurations du navigateur (restriction d'extension…) et à restreindre le téléchargement de certains fichiers, ainsi que les droits sur le poste de travail (droits administrateurs).

L'intégrité et la confidentialité des informations qui sont transmises sur Internet ne peuvent être garanties.

De ce fait, les utilisateurs doivent être conscients que les informations transitant sur Internet peuvent, à tout moment, être interceptées par des tiers, et doivent veiller à la fiabilité des sites consultés ainsi qu'à la sensibilité des informations échangées.

L'utilisateur doit être particulièrement vigilant lors des navigations effectuées sur Internet tant en matière de vérification de l'exactitude des données consultées qu'en matière de risque de corruption du SI.

Forums de discussion, blogs, réseaux sociaux

Il est rappelé que l'expression et la teneur des propos doivent être, à l'instar des autres modes d'expression, compatibles avec l'obligation de discrétion et le devoir de réserve qui s'imposent à chaque agent au titre des règles de déontologie.

Dans tous les cas, sauf accord explicite de la hiérarchie, les propos tenus ne pourront engager que leurs auteurs et toute allusion ou déclaration d'appartenance à l'Institution lors de publication sera proscrite.

La participation des agents avec leur adresse électronique professionnelle (adresse électronique en « paris.fr ») à des sites, forums ou blogs, réseaux sociaux contraires à l'ordre public, aux bonnes mœurs ou en contradiction aux principes d'éthique adoptés par la Ville de Paris est prohibée.

Communications audiovisuelles et messageries instantanées

Les outils de communication audiovisuelle (téléphonie, visio-conférence, messageries instantanées) mis à disposition par le Service Informatique sont à privilégier à l'ensemble des outils de communication audiovisuelle grand public que ces derniers soient chiffrés ou non (WhatsApp, Messenger, Viber …).

L'échange d'informations confidentielles est interdit sur tout autre outil de communication audiovisuelle que ceux fournis par le service informatique.

Moteurs de recherche et outils d'intelligence artificielle générative et agentique

Depuis de nombreuses années, des moteurs de recherche permettent de faire des recherches sur Internet en langage naturel.

A partir de 2022, de nouveaux outils d'intelligence artificielle, dite générative, sont apparus sur Internet (ChatGPT…). Ils sont capables, sur demande en langage naturel, de créer du contenu (texte, images, musique…). Désormais, des outils d'intelligence artificielle dite « agentique » permettent d'aller encore plus loin en effectuant des tâches de plus en plus complexes (raisonner, interagir avec des outils,…).

L'utilisation de l'IA générative et de l'IA agentique obéit à une doctrine d'usage fondée sur des principes simples qu'il convient de respecter :

- Se former à l'IA générative est encouragé. En particulier via les contenus mis à disposition par la DRH.
- Sécuriser les données de la ville : utiliser les outils mis à disposition par la ville, et non un outil grand public de façon à protéger les données de la Ville,

- Être transparent : signaler de façon visible s'il a été fait usage d'une IA pour produire un document ou une tâche,
- Conserver un esprit critique sur le résultat proposé : une IA donne par construction un résultat probable, pas nécessairement la vérité. L'expertise humaine reste donc nécessaire,
- Choisir le bon outil : limiter l'utilisation de l'IA générative et agentique aux cas où elle apporte une vraie plus-value.

Rester prudent sur les données confiées à une IA générative. En particulier, ne pas interroger une IA générative avec des données personnelles d'agents ou de citoyens.

Fiche 10 : La bonne utilisation de la messagerie professionnelle

Conseils généraux

L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée qu'un courrier manuscrit et qu'il peut, de plus, être rapidement communiqué à des tiers.

Avant tout envoi, il est impératif de vérifier l'identité des destinataires du message et de s'assurer de leur qualité à recevoir communication des informations transmises.

L'utilisateur doit sélectionner uniquement les personnes légitimes à recevoir les informations, que ce soit, dans le cadre d'une réponse à un message collectif ou lors d'un envoi à une liste de diffusion.

S'il reçoit un message électronique qui ne lui est pas destiné, l'utilisateur doit en informer l'émetteur, si celui-ci est également un utilisateur du SI de la Ville de Paris. Dans tous les cas, il doit veiller à effacer le message de son ordinateur et, dans la mesure du possible, ne pas le lire.

En cas d'envoi à une pluralité de destinataires, l'utilisateur doit éviter de diffuser des messages à un nombre important de destinataires afin de ne pas provoquer une saturation du service.

Il doit également envisager l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires (Cci).

Afin d'éviter tout risque de corruption du SI, l'utilisateur ne doit jamais sauvegarder ou ouvrir des pièces jointes suspectes.

Si un message électronique contenant une pièce jointe suspecte est reçu, le message doit être effacé immédiatement sans être ouvert. En cas de doute, les utilisateurs doivent contacter l'expéditeur du message s'ils le connaissent.

Afin d'éviter toute sollicitation intempestive (pourriel entre autres), il est demandé à chaque utilisateur de ne jamais utiliser son adresse professionnelle Ville de Paris sur des sites non professionnels.

L'utilisateur ne doit pas répondre à des messages non sollicités (pourriels) et ne doit pas envoyer ou faire suivre un message non sollicité tels que les pourriels, les canulars ou les « chaînes de lettres » ou « chaînes de solidarité ».

Aucune réponse ne doit être apportée aux messages électroniques demandant des informations personnelles.

L'hameçonnage est une technique qui consiste à envoyer de faux messages électroniques aux internautes, en leur faisant croire qu'ils émanent d'un tiers de confiance (banque, administration, support informatique, etc.) afin de récupérer leurs informations confidentielles tels que leurs mots de passe ou leurs coordonnées bancaires et ce, à des fins illégales. Cette fraude peut être réalisée à travers tous types de média électroniques (messagerie électronique, sites Internet, etc.).

Les messages d'hameçonnage doivent être signalés et transférés au service informatique à l'adresse d'alerte de mails frauduleux suivante mailsuspect@paris.fr de façon à ce que ce dernier puisse prendre les mesures adéquates (blocage de l'expéditeur, alerte...).

En cas d'absence, l'agent, utilisateur de la messagerie, active la fonctionnalité adéquate.

En cas d'absence d'un utilisateur et en cas de nécessité, un message d'absence sera mis en place par le Service informatique sans accès à sa messagerie.

En cas d'absence d'une durée susceptible de porter atteinte à la continuité de service ou en cas de nécessité absolue, sur demande de sa direction au Service informatique, la messagerie de l'utilisateur pourra être consultée par son responsable pendant une période limitée, avec pour unique objectif de lui permettre de récupérer les informations nécessaires à la poursuite de l'activité. L'utilisateur est informé par sa direction de cette opération qui est réalisée dans le respect de la correspondance privée. La correspondance privée doit être identifiée avec la mention "personnel" dans le champ de l'objet du mail.

L'utilisateur doit veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne doivent comporter aucun élément illicite, tel que des propos diffamatoires, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire.

L'utilisateur est responsable du contenu et de la forme de tout message qu'il émet avec son adresse de messagerie professionnelle.

Il ne doit pas se faire passer pour une autre personne en utilisant son adresse mail et ne doit pas modifier les documents reçus. Tout message envoyé depuis l'adresse professionnelle de la Ville de Paris associe nécessairement l'Institution à son contenu. L'utilisateur doit donc veiller à ce que celuici ne porte pas atteinte à l'image ou à la réputation de la Ville de Paris.

De manière générale, les informations confidentielles ou sensibles doivent être échangées en toute sécurité.

Ainsi :

- le transfert de ces informations vers des messageries n'appartenant pas à la Ville de Paris est strictement interdit,
- la redirection automatique de la boîte aux lettres professionnelle de la Ville de Paris vers toute autre boîte aux lettres électronique est prohibée.

Les informations sensibles ne doivent jamais être échangées à travers les messageries instantanées non professionnelles.

Utilisation de Smartphones personnels pour l'accès à la messagerie professionnelle

L'utilisateur peut accéder à la messagerie professionnelle à partir de smartphones personnels.

Ces périphériques peuvent induire des risques pour les données du SI et le respect de certaines précautions s'impose : Code pin, code de verrouillage, vérifications des applications, etc.

L'utilisateur est pleinement responsable de l'usage qu'il fait de ce type d'accès à la messagerie professionnelle. Il est particulièrement responsable de la protection des messages ou pièces jointes récupérées et stockées sur ce type de périphérique. Il veillera à en limiter l'accès par une protection adéquate (chiffrement, code de verrouillage).

Il signalera toute perte et tout vol.

Il apportera une vigilance toute particulière pour éviter toute fuite de données notamment en interdisant toute sauvegarde automatique des messages professionnels sur des ressources externes non gérées par la Ville de Paris.

En effet certaines offres commerciales incluent la mise à disposition de systèmes de sauvegarde ou de partage de données (Drive/Store). L'utilisateur, s'il n'y prête pas attention et ne configure pas correctement ces services, peut involontairement provoquer une fuite de données.

Limites et contraintes techniques

L'envoi de messages électroniques n'est possible, directement, que vers un nombre limité de destinataires, fixé par le Service Informatique.

De même, la taille, le nombre et le type des pièces jointes peuvent être limités par le Service Informatique pour éviter l'engorgement du système de messagerie.

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les agents sont invités à informer le Service Informatique des dysfonctionnements qu'ils constateraient dans le dispositif de filtrage.

III. Préconisations pour un usage responsable du système d'information

Fiche 11 : Numérique responsable et qualité de vie au travail

Numérique responsable

L'utilisateur doit faire preuve de sobriété dans ses usages des outils informatiques. En particulier, il doit suivre les bonnes pratiques suivantes :

- Limiter la luminosité des écrans ;
- Débrancher les chargeurs lorsqu'ils ne sont pas utilisés pour recharger un appareil ;
- Être sobre lors de l'accès à des sites internet consultés régulièrement : copier directement l'url dans la barre d'adresse, utiliser des favoris ou l'historique de navigation, et non systématiquement les moteurs de recherche ;
- Trier régulièrement sa boîte mail et ne pas y conserver les pièces jointes volumineuses ainsi que les mails qui ne servent plus ;
- Supprimer les fichiers stockés localement ou sur les répertoires réseaux lorsqu'ils ne sont plus utiles, dans le respect de la continuité de service et de la réglementation en termes d'archivage ;
- Lors d'une visioconférence, activer sa caméra pour la prise de parole et privilégier l'audio le reste du temps afin d'économiser la bande passante ;
- Et toute autre bonne pratique visant à limiter le poids des usages du numérique dans l'environnement de la Ville de Paris, communiquée par le service informatique.

Lutte contre l'infobésité numérique

- Éviter d'inclure des pièces jointes volumineuses dans les mails et privilégier les outils de partage de documents, en s'inscrivant dans la démarche de lutte contre l'infobésite numérique que la Ville de Paris met en place progressivement ; à ce titre, en particulier limiter le volume de mails échangés, par exemple en utilisant avec discernement la fonction "répondre à tous" ;
- Faire preuve de civilité dans les usages des outils numériques.

L'équipement de tout agent tient compte de l'objectif de sobriété numérique. Cet équipement est précisé dans la doctrine matérielle communiquée par le service informatique à l'ensemble des directions de la ville. La doctrine privilégie le concept d'un équipement unique par agent.

Droit à la déconnexion

Depuis 2016, la Ville de Paris s'est dotée de règles visant à prévenir l'usage inapproprié du numérique et à maîtriser son impact sur la sphère privée. Ces règles ont été précisées à l'occasion de l'adoption du nouveau règlement du temps de travail, entré en vigueur en 2022, dans une annexe dédiée, la "charte de la déconnexion et du bon usage des outils numériques" fondée sur cinq principes :

- Le respect des plages de travail,
- Le respect des plages de repos des interlocuteurs,
- La primauté des échanges vocaux,
- L'attention aux contenus des messages et aux destinataires,
- La responsabilité particulière des encadrants.

Fiche 12 : Matériel personnel, matériels non gérés par le service informatique

La connexion des matériels personnels (ou BYOD : Bring Your Own Device) des agents sur le réseau Intranet est interdite.

La connexion de matériels non gérés pas la Ville de Paris (ordinateurs de prestataires externes par exemple) doit être cadrée grâce à une procédure d'autorisation formalisée qui précisera également les conditions d'utilisation (dont solutions de sécurité obligatoires) et les limitations de ce type de service.

Le renvoi automatique de sa ligne professionnelle vers son téléphone personnel est interdit sauf nécessité impérieuse de service.

Fiche 13 : Les conditions d'utilisation du système d'information à des fins personnelles (vie privée résiduelle)

Les ressources informatiques mises à la disposition des utilisateurs sont destinées à un usage professionnel.

Dans le cadre des nécessités de la vie courante, un usage personnel modéré et raisonnable est toléré, à condition qu'il soit conforme à la législation en vigueur et aux bonnes mœurs, et qu'il ne nuise pas aux tâches professionnelles incombant à l'utilisateur, à la sécurité du système d'information, ou à la bonne conduite des activités de la Ville de Paris.

Internet

Concernant Internet, l'utilisateur ne devra pas nuire à la qualité du débit en téléchargeant des fichiers volumineux ou en consultant des sites consommateurs de bande passante (vidéos, télévisions, radios …).

Téléphone professionnel

Comme pour les autres ressources, un usage personnel modéré et raisonnable du téléphone professionnel est toléré en zone Europe. La mise à disposition de double SIM ou eSIM est possible pour faciliter l'utilisation d'un même smartphone pour les usages personnels et professionnels. A l'international hors zone Europe, l'itinérance doit être désactivée impérativement.

Messagerie

Tout message reçu ou envoyé depuis le poste de travail mis à disposition par l'employeur a, par principe, un caractère professionnel.

Les messages à caractère personnel sont tolérés, à condition de respecter la législation en vigueur, de ne pas perturber et de respecter les principes posés dans la présente charte.

Les messages à caractère syndical, à large diffusion, ne peuvent pas être envoyés à partir de la messagerie professionnelle. Les agents n'ont donc pas le droit d'en transmettre, ni retransmettre. Seules les organisations syndicales ont la possibilité de diffuser une information syndicale dans le respect du protocole d'accord entre la Ville de Paris et les organisations syndicales. Ce protocole prévoit notamment que tout message à destination des agents doit partir de l'Intranet et non de la messagerie, d'une part, et que chaque agent doit pouvoir choisir de recevoir ou de ne pas recevoir l'information syndicale, d'autre part. Par conséquent, l'information syndicale doit comprendre la possibilité de se désabonner.

Tous les messages électroniques émis, reçus ou stockés depuis le SI et non identifiés comme étant personnels sont, par défaut, considérés comme étant professionnels et appartenant à la Ville de Paris.

Ainsi, chacun doit veiller à clairement identifier la nature personnelle d'un message en indiquant la mention « Personnel » dans l'objet de celui-ci, ou en le stockant dans un répertoire portant cette même mention. Il est néanmoins strictement interdit de transformer ou qualifier un message de nature professionnelle en message privé.

En cas de saturation de la boite de messagerie, les messages personnels devront être supprimés par l'utilisateur. Si ces actions ne sont pas réalisées, une suppression automatique et définitive peut être effectuée. Une information préalable sera faite auprès des utilisateurs.

Les messages contenus dans les dossiers des éléments supprimés ou les dossiers des courriers indésirables pourront être automatiquement supprimés.

Le détail et les modalités de mise en œuvre de ces actions sont disponibles sur l'intranet du Service Informatique.

Espace de stockage

En l'absence d'indication contraire, toute information est considérée par défaut comme étant professionnelle et appartenant à la Ville de Paris.

Les informations ou documents personnels doivent donc être clairement identifiés soit en indiquant la mention « Personnel » soit en les stockant dans un répertoire portant cette même mention.

De plus, l'utilisateur ne doit en aucun cas transformer ou qualifier des documents de nature professionnelle en documents personnels.
Si l'espace d'un disque est saturé par des données personnelles, l'utilisateur devra supprimer ces données. Si cette action n'est pas effectuée, une suppression définitive pourra être effectuée après information préalable faite auprès des utilisateurs.

Responsabilité

L'utilisateur est entièrement responsable de la gestion de ses données personnelles. L'utilisateur ne pourra tenir pour responsable la « Ville de Paris » des incidents survenant à ses données personnelles (perte de fichiers suite à une panne matérielle par exemple, ou suppression suite à une infection virale).

Départ d'un utilisateur

L'utilisateur est responsable de son espace à caractère privé.

En cas de départ de la Ville de Paris, l'utilisateur est informé de la date de clôture de son compte et il lui appartient de récupérer puis supprimer ses données personnelles (y compris celles de messagerie). Il veille à ne pas supprimer d'informations professionnelles lors de ces opérations.

Le compte de l'utilisateur partant est désactivé et le contenu professionnel de la boite de messagerie sera conservé pour une période maximale de trois mois afin d'assurer la continuité de service.

L'utilisateur a obligation de restituer tous les matériels informatiques de la Ville de Paris.

A défaut, la Ville de Paris peut émettre à son encontre un titre de recette correspondante à la valeur de l'équipement.

IV. Opérations de contrôle et de suivi

Fiche 14 : Les types de contrôle

Contrôles automatisés

Le système d'information et de communication s'appuie sur des fichiers journaux (" logs "), créés en grande partie automatiquement par les équipements informatiques et de télécommunication. Ces fichiers sont stockés sur les postes informatiques et sur le réseau. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations de l'entreprise, en détectant des erreurs matérielles ou logicielles et en contrôlantles accès et l'activité des utilisateurs et des tiers accédant au système d'information.

Les utilisateurs sont informés que de multiples traitements sont réalisés afin de surveiller l'activité du système d'information et de communication.

Sont notamment surveillées et conservées les données relatives :

- À l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications ou suppressions de fichiers,
- Aux connexions entrantes et sortantes au réseau interne, à la messagerie et à Internet, pour détecter les anomalies liées à l'utilisation de ces ressources et surveiller les tentatives d'intrusion et les activités, telles que la consultation de sites web ou le téléchargement de fichiers.

L'attention des utilisateurs est attirée sur le fait que des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements et afin de renforcer la sécurité du système d'information, dans le respect des règles en vigueur.

Ainsi, le service informatique peut être amené, entre autres, à surveiller et à analyser de manière globale comme de manière individuelle :

- L'utilisation d'internet,
- L'utilisation de la messagerie électronique,
- L'utilisation des téléphones et télécopieurs,
- L'utilisation des imprimantes,
- L'accès aux postes de travail et aux applications ainsi que les actions effectuées,
- Les accès aux répertoires partagés ou aux bases collaboratives.

Ces contrôles ont pour objectif de :

- S'assurer que les procédures et les politiques de la Ville de Paris sont bien respectés et ainsi contrôler tout abus,
- Surveiller les niveaux de service et les performances de ses ressources matérielles,
- Veiller à ce que les ressources ou outils payants et d'utilisation nominative sont effectivement utilisés,
- Se conformer aux obligations légales.

Ces traces techniques sont conservées pour une période maximale d'un an.

Cette surveillance s'exerce dans le respect du Règlement Général sur la Protection des Données (RGPD) et aux dispositions du Code des Postes et des Communications Électroniques.

Tous les traitements de données nominatives opérés par le service informatique font l'objet de déclaration au registre des traitements de la collectivité et sont contrôlés par le Délégué à la Protection des Données.

Procédures résultant d'obligations légales

La Ville de Paris est dans l'obligation légale de mettre en place un système de journalisation des accès Internet, de la messagerie et des données échangées.

Les traces nécessaires pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales sont conservées un an conformément à la législation en vigueur.

Procédures de contrôle manuel

En cas de dysfonctionnement technique constaté par le Service Informatique, il peut être procédé à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs utilisateurs.

Lorsque le contrôle porte sur les fichiers d'un utilisateur et, sauf risque ou événement particulier, le Service Informatique ne peut ouvrir les fichiers identifiés par l'agent comme personnels sauf en présence de ce dernier.

Le contenu des messages à caractère personnel des utilisateurs ne peut en aucun cas être contrôlé par le Service Informatique.

En cas de risque ou événement particulier, notamment pour assurer la sécurité du Système d'Information, la Ville de Paris peut être amenée à consulter les traces nominatives et les informations personnelles des utilisateurs en présence du propriétaire des informations concernées ou à défaut après l'avoir prévenu.

Fiche 15 : Les possibles limitations à l'utilisation des ressources

Si une utilisation à usage personnel est tolérée, elle ne doit pas être contraire à l'ordre public ni compromettre l'intérêt et la réputation de la Ville de Paris. Elle ne doit pas rentrer en conflit avec la qualité de service (débit, bande passante, limitation de la capacité des ressources) et elle ne doit pas nuire à la conduite des activités professionnelles.

Dans le cadre de sa maîtrise de l'allocation des ressources et de sa politique de sécurité du réseau, la Ville de Paris se réserve le droit de poser des limites à l'utilisation d'internet ou de la messagerie tels que la mise en place de dispositifs de filtrage de sites non autorisés ou l'interdiction de téléchargement ou de connexion.

Des outils de contrôle de la messagerie tels que les outils de détection de virus ou filtres anti- spam sont mis en œuvre.

Un usage anormal des moyens informatiques mis à disposition, et contraire aux règles posées par la présente charte, sera susceptible d'entraîner des sanctions disciplinaires en application des règles qui les régissent.

À noter également que dans le but de maitriser sa consommation téléphonique, un logiciel de collecte permet aux directions d'avoir accès pour l'ensemble de leur direction mais également pour chaque agent à des indications sur la durée et le cout mensuel des communications.

Dans le but de maitriser les dépenses associées aux logiciels souscrits par abonnement de façon nominative (Teams, mail agent de terrain, Digdash, Autocad... et les logiciels nécessitant un abonnement individuel payant), un traitement collecte les données d'usage de ces logiciels. Le service informatique et les services informatiques en direction sont habilités à consulter la liste des utilisateurs dotés de ces logiciels et pourtant inactifs depuis trois mois pour deux finalités :

- Suspendre les abonnements inutiles,
- Accompagner les agents qui auraient besoin d'aide pour la prise en main de ces outils.

Enfin, pour encourager la transformation numérique, le service informatique collecte les données relatives à l'utilisation des boîtes aux lettres électroniques ; laquelle permet ensuite, dans le cadre de la médiation numérique, et en relation avec les directions, de suivre et d'accompagner les agents dans l'utilisation des outils numériques.

Fiche 16 : Le contrôle de l'Inspection générale de la Ville de Paris

La délibération 2014-IG-1001 du Conseil de Paris du 16 juin 2014 définissant les missions et les conditions d'intervention de l'Inspection générale de la Ville de Paris dispose que ses membres « doivent avoir libre accès, dans les services, aux documents, pièces et fichiers de toutes natures qui ont un lien avec l'objet de leur mission. »

Il résulte de ces dispositions que l'Inspection générale, dans le cadre des investigations administratives qu'elle réalise à l'occasion des missions dont elle est chargée par la Maire, est habilitée à accéder aux contenus du système d'information de la Ville de Paris mais également à analyser l'utilisation qu'un ou des agents ont pu en faire à titre individuel. Elle doit établir à cet effet une demande formelle au responsable du service informatique.

V. Signalement d'incidents

Fiche 17 : La vigilance de chaque utilisateur

Toute anomalie suspectée ou avérée concernant le SI de la Ville de Paris (vols ou pertes de matériel, vols ou pertes d'Informations, dysfonctionnements du poste de travail, incident sur une application), ou toute violation des règles décrites dans la présente charte, doit être signalée au support SI ou à au responsable hiérarchique, qui traiteront l'incident.

Concernant le cas plus spécifique de fuite de données personnelles, le Délégué à la protection des données (DPD) doit être informé sans délai.
Les messages d'hameçonnage doivent être signalés et transférés au service informatique à l'adresse d'alerte des mails frauduleux suivante mailsuspect@paris.fr de façon à ce que ce dernier puisse prendre les mesures adéquates (blocage de l'expéditeur, alerte, …) (cf. fiche 10).

VI. Sanctions

Fiche 18 : Les conséquences du non-respect de la Charte

Par les agents de la Ville

En cas de violation avérée des politiques et des règlements en vigueur et des dispositions de la présente charte, la Ville de Paris se réserve le droit d'engager des procédures disciplinaires à l'encontre de leurs auteurs, sans préjudices d'éventuelles sanctions judiciaires.

Par ailleurs, la Ville de Paris pourra procéder à la suspension des droits d'accès de l'utilisateur au SI.

Par les salariés d'un prestataire

Concernant les utilisateurs liés par un contrat de prestation ou une convention avec la Ville de Paris, tels que les intérimaires, les partenaires ou les fournisseurs, toute violation des règles édictées par la présente charte, hors cadre dérogatoire, peut entraîner la rupture dudit contrat voire des poursuites judiciaires à l'égard de l'entreprise d'origine ou de la personne concernée.

La procédure en cas de doute

En cas de doute sur la légalité d'une opération, les utilisateurs peuvent consulter les services de documentation qui mettent à leur disposition des ouvrages et des textes de lois, ou consulter le Code de la Propriété Intellectuelle sur le site Internet www.legifrance.gouv.fr

Pour tout conseil pour l'application de la présente charte, il est possible de s'adresser à la Direction des systèmes d'information et du numérique par l'intermédiaire de votre Correspondant Informatique et à la Direction des affaires juridiques, par l'intermédiaire du Correspondant Juridique de son entité.