Charte pour le bon usage des systèmes d'information et de télécommunication de la Ville de Provins

Conseil municipal du 4 avril 2025
Délibération n° 2025.26

Table des matières

ARTICLE 1 - PREAMBULE

La présente charte rappelle les règles d'utilisation des moyens informatiques et téléphoniques de la ville de Provins afin de favoriser un usage optimal de ces ressources en termes de sécurité, de confidentialité, de performance, de respect de la réglementation et des personnes.
Elle a pour finalité de contribuer à la préservation de la sécurité du système d'information de la collectivité et fait de l'utilisateur un acteur essentiel à la réalisation de cet objectif.

De façon pragmatique, elle permet d'informer l'agent sur :

- Les usages permis des moyens informatiques mis à sa disposition ;
- Les règles de sécurité en vigueur ;
- Les mesures de contrôle prises par l'employeur ;
- Les sanctions encourues.

Ce règlement s'applique à l'ensemble des agents, tous statuts confondus, aux élus, stagiaires, visiteurs, et plus généralement à tous les utilisateurs des moyens informatiques et téléphoniques de la collectivité.
L'ensemble des devoirs de l'utilisateur prévu par la charte doit conduire ce dernier à adopter un comportement responsable vis-à-vis du système d'information de la collectivité.

ARTICLE 2 - DEFINITIONS

On désignera de façon générale sous le terme « moyens informatiques », les ressources informatiques de calcul ou de gestion locales, ainsi que celles auxquelles il est possible d'accéder à distance, directement ou en cascade, à partir du réseau administré ou utilisé par la ville de Provins.
On désignera par « moyens téléphoniques », tous les téléphones fixes ou portables, radiotéléphones, assistants personnels, fax, modems mis à disposition par la ville pour l'exercice de l'activité professionnelle.
On désignera par « services Internet/Intranet », la mise à disposition par des serveurs locaux ou distants, de moyens d'échanges et d'informations diverses : site web, messagerie, forum…
L'activité professionnelle est celle qui est nécessaire, utile, dépendante ou complémentaire à l'activité des services municipaux, quelle qu'en soit la nature.

ARTICLE 3 - ACCES AUX RESSOURCES INFORMATIQUES, SERVICES INTERNET/INTRANET ET MOYENS TELEPHONIQUES

3.1 UTILISATION DES RESSOURCES

Les ressources informatiques, l'usage des services Internet/Intranet et du réseau pour y accéder,ainsi que les moyens téléphoniques, sont exclusivement mis à disposition des utilisateurs (tels que définis à l'article 5 de la présente charte) afin de permettre :

- L'exercice des activités des agents de la ville de Provins ou des services offerts à la population
- Les prestations demandées par la ville de Provins à ses prestataires, même occasionnels (ex : stagiaires)

L'utilisation de ces ressources est strictement réservée à un usage professionnel : aucun usage à des fins personnelles n'est donc admis.

3.2 RESPONSABILITES

L'utilisateur est informé que sa propre responsabilité, celle de son chef de service, et la responsabilité de la collectivité peuvent être engagées civilement et pénalement du fait de son comportement. Il veillera donc à respecter les lois et règlements en vigueur, notamment ceux mentionnés à l'article 6, ainsi que les règles d'utilisation, de sécurité et de bons usages décrits dans la présente charte.

3.3 PRISE DE MAIN ET OBSERVATION A DISTANCE

Le service informatique dispose d'outils de prise de main à distance qui sont généralement employés pour dépanner les utilisateurs, en leur montrant directement les manipulations qu'ils ont àfaire. Ces prises de main et observations à distance se feront toujours avec l'accord de l'intéressé.

3.4 ABSENCE DE L'AGENT

En cas d'absence de l'agent, la continuité du service doit être assurée. L'agent doit veiller à ce que le service puisse accéder aux documents, logiciels et dossiers indispensables à l'activité (transmission des documents et dossiers aux collègues, ou mise à disposition dans un dossier partagé, création de comptes pour accéder aux applications, à l'exclusion de toute communication de mots de passe personnels). Si l'absence est imprévue (maladie, accident), le supérieur hiérarchique pourra demander au service informatique l'accès à l'espace de travail de l'agent. En cas de départ définitif ou de mutation, le successeur récupère les documents de travail ainsi que les messages électroniques.

ARTICLE 4 - REGLES D'UTILISATION, DE SECURITE ET DE BON USAGE

Tout utilisateur est responsable du bon usage des équipements mis à sa disposition. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale.
L'utilisation de ces ressources doit être rationnelle et loyale afin d'éviter leur saturation ou leur détournement à des fins personnelles.
En particulier, l'utilisateur doit appliquer les recommandations suivantes :

4.1 SECURITE DES DONNEES ET DU RESEAU

4.1.1 Mots de passe

Chaque utilisateur se voit attribuer un identifiant et un mot de passe, ainsi que des habilitations en fonction de ses besoins (accès internet, accès aux applications, accès à des serveurs, applications hébergées, ressources numériques etc.).
Les habilitations des utilisateurs peuvent changer selon l'évolution de leurs fonctions, de leurs rôles et de leurs appartenances (services). Tout changement de fonction, de rôle ou d'appartenance doit être notifié au service informatique par l'entité responsable de l'utilisateur.
Les accès sont révoqués et le compte utilisateur supprimé dès lors que l'agent cesse ses fonctions pour la collectivité.

Il convient de s'identifier clairement et d'utiliser des mots de passe pour protéger l'accès à ses matériels et programmes.

Ces mots de passe doivent être stockés dans des coffres-forts numériques prévus à cet effet et ne doivent pas être conservés sur les postes de travail des utilisateurs sur des supports non cryptés (EX : fichier Word ou Excel). Ils peuvent également être stockés sur support papier sous réserve qu'ils soient conservés de manière sécurisé (ex : Tiroir fermé à clé, coffret fort, etc…).
Ces mots de passe ne doivent pas être communiqués ni notés sur des supports accessibles à autrui.
Ils ne doivent pas être faciles à deviner par une personne mal intentionnée (pas de prénoms ou dates de naissance de proches, par exemple) et doivent respecter les exigences de complexité suivantes :

- Ils doivent comporter au moins 15 caractères,
- Ils doivent comporter au moins une majuscule, une minuscule, un chiffre et un caractère spécial
- Ils doivent être changés au moins une fois par an, en évitant de reprendre ceux qui ont déjà été utilisés

L'usage des technologies de biométrie (reconnaissance faciale, empreinte digitale), couplé à un mot de passe respectant les exigences de complexité est toléré.
Pour des raisons de sécurité, le service informatique se réserve le droit d'imposer un changement régulier des mots de passe.
Les mots de passe sont personnels et chaque utilisateur est responsable de l'utilisation qui peut en être faite : il ne devra en aucun cas transmettre à des tiers les moyens d'authentification qui lui sont fournis par la collectivité, lesquels doivent rester personnels et confidentiels.
L'emploi de mots de passe communs à plusieurs personnes est interdit. Néanmoins, cette disposition ne s'applique pas lorsque les comptes ou les ordinateurs sont liés à une fonction ou à une structure (exemple : messagerie d'un service, guichet).

Seules les personnes du service informatique peuvent exceptionnellement être amenées à utiliser un mot de passe d'un utilisateur, avec son accord, pour résoudre un problème que ce dernier leur aura signalé.
L'utilisateur ne communiquera aucun mot de passe au téléphone s'il n'est pas absolument sûr de l'identité et de l'habilitation de son interlocuteur. En cas de doute, il devra rappeler la personne au service informatique (numéro interne), pour poursuivre l'opération.
Enfin, lorsque que cela est possible techniquement, les mécanismes d'authentifications à double facteur doivent être systématiquement privilégiés par les agents, et ce, pour tous types d'usages (Exemple : portail internet, accès à la messagerie à travers le Webmail, etc…)
Ce mécanisme permet d'utiliser un n° de téléphone, une adresse mail ou une application de sécurité afin de communiquer un code personnel à usage unique lors d'un renouvellement de mot de passe, ou lors de l'authentification sur certains systèmes sensibles.

4.1.2 Usurpation d'identité

Ne pas tenter de masquer sa véritable identité ou d'usurper l'identité d'une autre personne pour essayer d'accéder à ses informations ou ses traitements.
Les courriels sont notamment protégés par le secret de la correspondance. Nul ne peut en prendre connaissance sans autorisation de l'émetteur ou du destinataire, à l'exception d'un juge d'instruction ou d'un officier de police judiciaire, qui peut, en cas de plainte, procéder à la saisie desdonnées nécessaires à la manifestation de la vérité.
Il convient de signaler au service informatique toute tentative d'accès anormal à son poste de travail et, de façon générale, toute anomalie que l'on peut constater.

4.1.3 Données d'autrui

Ne pas tenter de lire, modifier, copier ou détruire des données autres que les siennes. En particulier, ne pas modifier de fichiers contenant des informations comptables ou d'identification, ni tenter de prendre connaissance d'informations détenues par d'autres utilisateurs, même si ceux-ci ne les ont pas explicitement protégées, exception faite des données diffusées dans des dossiers publics ou partagés qui sont clairement identifiés.
Il est expressément rappelé qu'accéder sans autorisation à des informations d'autres utilisateurs, les copier, les divulguer, les modifier ou les effacer, peut être sanctionné pénalement.

4.1.4 Informations confidentielles – registre des traitements

Ne pas divulguer d'informations confidentielles, notamment par téléphone, à des tiers qui ne doivent pas les connaître. En particulier, les traitements ou fichiers concernant des informations relatives à des personnes (nom, numéro…) doivent être répertoriés dans le registre des traitements de la collectivité dans le cadre du RGPD ; ce registre stipule notamment les finalités exactes des traitements, la liste des destinataires des diverses informations, ainsi que leur durée de conservation.

Le service informatique vous assiste dans l'établissement de ces fiches de registre.

La loi Informatique et libertés du 6 janvier 78 modifiée fixe un ensemble de contraintes pour ces traitements : respect des finalités et des durées de conservation déclarées, information des personnesconcernées, qui ont aussi un droit d'accès et de rectification aux données les concernant, accès sécurisé aux données et obligation de sauvegardes…

Les fichiers non automatisés (papier) dont les informations proviennent ou sont appelées à être enregistrées dans ces traitements, sont soumis aux mêmes contraintes, et doivent donc être utilisés avec les mêmes précautions.

4.1.5 Accès aux postes de travail

Ne pas laisser des ressources ou services accessibles à des tiers en cas d'absence du poste de travail ; mettre l'ordinateur en veille ou verrouiller le poste avant de s'absenter, même momentanément.

La mise en fonction automatique de l'économiseur d'écran, au bout de 20 minutes d'inactivité est activée, avec saisie obligatoire d'un mot de passe pour quitter la veille.

Veiller à ce que les impressions ou sauvegardes contenant des informations sensibles ou nominatives (noms, adresses, photos de personnes…) ne soient pas accessibles à des personnes non autorisées (conservation obligatoire sous clé dans les bureaux recevant du public). Également, tout support (papier, CDROM…) doit être rendu illisible avant mise au rebut.

4.1.6 Sauvegardes

Effectuer régulièrement la sauvegarde de ses données en utilisant les moyens mis à disposition, et garder un exemplaire des courriels et documents bureautiques reçus ou produits dans le cadre de l'exercice de ses fonctions, dans un but d'archivage légal, au même titre que les documents papier.

Attention, les sauvegardes des traitements automatisés de données nominatives doivent tenir compte des durées de conservation déclarées : il convient donc de veiller à ce que ces durées de conservation soient respectées en supprimant ou en anonymisant les données périmées dans les traitements, mais également les sauvegardes, les exports et les états, quel qu'en soit le support (disque dur, serveur de fichier, papier). Néanmoins, si ces données à caractère personnel ont une utilité administrative, un intérêt statistique ou historique, elles sont à transférer au service des archives qui les prend en charge, ou autorise leur destruction.

La sauvegarde de fichiers professionnels sur des outils non fournis par la collectivité n'est pas autorisée.

4.1.7 Téléchargement et installation de logiciels

Ne pas télécharger, installer, utiliser ou contourner les restrictions d'utilisation d'un logiciel pour lequel la mairie n'a pas acquis de licence. Seules les personnes du service informatique sont habilitées à installer des logiciels, y compris des logiciels libres, et utilisent pour cela des comptes d'administrateurs sur les machines. Les autres utilisateurs disposent de comptes d'utilisation restreints qui sont suffisants pour un usage courant.

Tous les logiciels doivent faire l'objet d'une demande officielle d'installation au service informatique qui en définira les modalités.

4.1.8 Droits de reproduction

Ne pas copier un logiciel pour l'utiliser sur un autre poste, ou en dehors de son lieu de travail. Les copies de sauvegarde de logiciels, prévues par le code de la propriété intellectuelle, sont exclusivement effectuées par le service informatique, sauf dans le cas de l'acquisition directe d'un logiciel par un autre service.
Des droits de reproduction existent également pour les œuvres littéraires, musicales, photographiques, audiovisuelles, qui ne doivent en aucun cas être téléchargées sur internet, reproduites ou diffusées sans autorisation de l'auteur, ou du propriétaire des droits d'exploitation.

4.1.9 Photographies, droit à l'image

L'image d'une personne ne peut être utilisée ou diffusée sans son consentement écrit (celui de son responsable légal pour un mineur). D'une manière générale, les photos que les agents peuvent être amenés à prendre dans l'exercice de leurs fonctions ne doivent donc pas comporter de personnes, plaques d'immatriculation, enseignes de magasins : il est recommandé de flouter ces éléments.
Les photos prises dans le cadre des activités de la mairie de Provins ou dans ses locaux ne peuvent pas être utilisées à des fins personnelles, et sont interdites à la diffusion externe sans le consentement écrit de la Direction Générale. Cette recommandation s'applique aux enregistrements vidéo et sonores.

4.1.10 Equipements étrangers

Ne pas connecter sans autorisation, à un poste ou au réseau, un équipement étranger à la collectivité (disques durs externes, souris, clavier, clé USB, smartphone ou téléphone personnel, etc…) et susceptible de provoquer des dysfonctionnements, ou d'introduire des virus informatiques.
Toute connexion d'un nouveau matériel doit se faire avec l'autorisation préalable du service informatique.

4.1.11 Messagerie

Ne pas ouvrir de pièce jointe d'un courriel dont on n'est pas absolument certain de la provenance et de l'innocuité. Si cette pièce jointe est un document contenant des macros (tels que Word ou Excel), ne pas permettre l'exécution de ces macros dans ce cas. Il est possible que des actions préjudiciables soient effectuées par ces macros (macrovirus).
La messagerie dispose d'un outil de filtrage qui élimine automatiquement tout message suspect, en entrée et en sortie. Sont également éliminés tous les messages considérés comme des « pourriels » (spam), et qui sont reconnus par la teneur du titre ou du corps du message.
Attention, ces filtres ne sont pas fiables à 100%. Il peut arriver que certains pourriels ne soient pas détectés ou que des messages légitimes soient écartés.
Les agents reçoivent tous les jours des courriels intitulés « Rapport de quarantaine », qui permettent de récupérer les messages écartés par le filtrage anti-spam, et en cas de doute, de prévisualiser de manière sécurisée les mails bloqués dans la quarantaine.
En cas de doute accru, l'agent pourra s'adresser au service informatique qui effectuera des vérifications.
Par ailleurs, une copie de tout message électronique entrant ou sortant est conservée pour une durée d'un mois et peut-être réémis à tout moment depuis la plateforme de filtrage. L'utilisation, à titre professionnel, de comptes de messagerie non gérés par la mairie de Provins est interdite.Les comptes professionnels se terminent obligatoirement en @mairie-provins.fr

▲ Remarque importante :
Un message électronique peut constituer une preuve, et peut engager fermement son expéditeur et son destinataire : il existe un risque réel pour qu'un agent prenne des engagements qu'il faudra ensuite respecter.
Toutes les recommandations concernant les échanges écrits avec des tiers s'appliquent donc à la messagerie.
L'envoi de messages électroniques doit respecter les mêmes procédures de contrôle, de validation, d'autorisation que les courriers.
Il est souhaitable de mettre systématiquement en copie des messages importants son responsable et le responsable du destinataire, et il est obligatoire de transmettre pour validation à un responsable tout message qui aurait valeur contractuelle ou d'engagement.

Par ailleurs, tout message important doit être conservé à des fins d'archivage.

4.1.12 Virus

L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes informatiques et des réseaux, que ce soit par des manipulations anormales du matériel ou par l'introduction de logiciels parasites connus sous le nom générique de virus, chevaux de Troie, bombes logiques…
Des comportements inhabituels d'un logiciel ou d'un ordinateur tels que l'ouverture de fenêtres intempestives, l'activité inexpliquée du disque dur ou la dégradation importante des performances peuvent traduire la présence d'un logiciel parasite : contacter rapidement le service informatique.

4.1.13 Anti-Virus

Le service informatique installe sur les machines un logiciel destiné à vous protéger des programmes malveillants. Cet outil ne doit pas être désinstallé, et il est paramétré pour se mettre à jour régulièrement (reconnaissance de nouveaux virus). Le paramétrage ne doit donc pas être modifié, et il est recommandé aux utilisateurs d'ordinateurs portables de se connecter régulièrement à internet pour que cette mise à jour puisse être effectuée.
Attention, en cas de détection de virus, un message du logiciel antivirus vous avertit : veuillez contacter immédiatement le service informatique.

4.1.14 Navigation internet

L'accès aux sites web jugés dangereux, illégaux, contraires à l'ordre public ou aux bonnes mœurs (site pornographique, discriminatoire, violent ou site de téléchargement illégal…) ainsi que certaines catégories non utiles à l'activité professionnelle des agents est interdit.
Afin de protéger son système d'information contre les risques inhérents à ce type d'usage, la collectivité a mis en place en amont, un dispositif de filtrage.
L'accès à internet à travers la navigation est contrôlé par un filtrage URL/Anti-virus (un serveur, appelé proxy filtrant, agit comme un intermédiaire entre l'utilisateur et le site Internet).
Lorsqu'un utilisateur tente d'accéder à un site, le proxy analyse la requête et compare l'URL du site avec une base de données conforme à la politique de filtrage de la collectivité.
Cette base de données, contenant une liste d'URL malveillantes, dangereuses ou interdites, permet au proxy d'autoriser ou de refuser l'accès :

- Si l'URL n'est pas répertoriée dans la base de données, le proxy autorise l'accès, car le site est jugé sûr
- Si l'URL est présente dans la base de données, l'accès est refusé, car le site est potentiellement dangereux.

Ce dispositif, permet également de répondre à une disposition légale qui consiste en l'obligation de conserver les logs de connexion des postes du réseau local à internet pendant une durée de 365 jours.

4.1.15 Gestion des mises à jour

Les appareils numériques et les logiciels utilisés au quotidien sont exposés à des failles de sécurité. Ces failles peuvent être utilisées par des cybercriminels pour prendre le contrôle d'un ordinateur ou d'un équipement mobile. Face à ces risques, les éditeurs et les fabricants proposent des mises à jour (patch en anglais) visant à corriger ces failles.
L'utilisateur doit donc approuver l'installation des mises à jour des équipements numériques de la collectivité dès qu'elles sont disponibles et proposées.

4.1.16 BYOD

Le BYOD (Bring Your One Device), est une pratique qui consiste à utiliser son matériel personnel dans le cadre professionnel. Par exemple, l'utilisation d'un ordinateur portable personnel pour travailler dans le cadre professionnel. Cette pratique est considérée par la collectivité comme étant à risque et est rigoureusement interdite.

4.2 REGLES MINIMALES DE COURTOISIE ET DE RESPECT D'AUTRUI

Il convient de faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques (courriels, forums de discussions…)

4.2.1 Opinions personnelles et propos illicites

Ne pas émettre d'opinions personnelles étrangères à son activité professionnelle, et susceptibles de porter préjudice à la collectivité. Sont notamment interdits la consultation, la rédaction, le téléchargement, l'enregistrement, l'envoi et la diffusion de messages, textes, images, films, pages web, etc. à caractère injurieux, raciste, antisémite, discriminatoire, insultant, dénigrant, diffamatoire, dégradant, pornographique, faisant l'apologie de crime, incitant à la haine…
De même, les propos susceptibles de révéler les opinions politiques, religieuses, philosophiques, les mœurs, la santé des personnes, ou encore de porter atteinte à leur vie privée ou à leur dignité, ainsi que les messages portant atteinte à l'image, la réputation ou à la considération de la ville de Provins sont à proscrire.

▲ Remarque : un agent ne peut être tenu pour responsable s'il reçoit de tels documents sans les avoir sollicités, mais il lui est demandé de les détruire sans délai.

4.2.2 Messages non sollicités

Veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés, afin d'éviter l'encombrement inutile de la messagerie et une dégradation des temps de réponse. Attention, les messages non sollicités (appels à la solidarité et autres chaînes) que leur auteur demande de diffuser à un maximum de personnes, sont généralement des canulars. En cas de doute, le service informatique pourra vous conseiller au mieux.

4.2.3 Emploi de la langue Française

Eviter l'emploi de termes en langue étrangère dans des courriers ou communications. Lorsque des termes français de même sens existent, leur emploi est obligatoire.

ARTICLE 5 - APPLICATION DE LA CHARTE & SANCTIONS

5.1 PERIMETRE D'APPLICATION

La présente charte s'applique à l'ensemble des agents de la ville de Provins, tous statuts confondus, aux élus, stagiaires, visiteurs, infogérant, sous-traitant et plus généralement à l'ensemble des personnes, permanentes ou temporaires, utilisant les moyens informatiques et téléphoniques de la ville de Provins.
Elle fera l'objet d'une large diffusion, tant collective qu'individuelle, par tout moyen utile (parapheur, messagerie, note de service, affichage…) afin que nul ne puisse en ignorer son existence et son contenu.
Ainsi, dès l'entrée en vigueur de la présente charte, chaque personne concernée et visée au présent article aura accès au texte de la version en vigueur. Elle devra en prendre immédiatement connaissance et sera tenue sans délai au respect des règles qui y sont édictées.

La présente version de la charte est répertoriée sous la référence indiquée en pied de page, et fera l'objet d'une présentation au comité social paritaire (CST).
Chaque nouvelle version sera validée et diffusée de la même manière. La version en vigueur sera la plus récente.

5.2 MANQUEMENT AUX REGLES ET MESURES DE SECURITE

Le manquement aux règles et mesures de sécurité de la présente charte informatique est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication.
La charte informatique étant un document de portée juridique, elle permettra de fonder les sanctions à l'encontre d'un utilisateur qui ne l'aurait pas respectée ; son non-respect peut donc entraîner l'application de sanctions disciplinaires, sans préjudice des autres poursuites envisageables (mise en cause de la responsabilité civile, mise en cause de la responsabilité pénale).

5.2.1 ABUS ET CONTROLES

L'utilisateur est informé que toute utilisation non professionnelle pourra faire l'objet de sanctions. De ce fait, il reconnaît avoir été averti que le système d'information de la ville fait l'objet d'une surveillance constante (serveurs, réseaux, postes de travail, téléphones, logiciels, virus…), et qu'en cas de comportement suspect, certains équipements sont soumis à une surveillance particulière, notamment sur les volumes d'informations traitées (enregistrement, téléchargement), les durées anormales d'utilisation, les connexions à des sites internet prohibés ou les tentatives d'intrusions.

Ainsi sont conservées de manière automatique les informations suivantes :

- L'adresse (appelée URL, par exemple www.mairie-provins.fr) et l'heure de toute connexion à un site web depuis un ordinateur du réseau local de la collectivité (identifié par une adresse IP telle que 100.100.100.x) pendant une durée de 365 jours.
- Une copie de tout courrier électronique réceptionné et émis par le serveur de messagerie de la collectivité, y compris les courriels non sollicités (SPAM) pour une durée d'un mois.
- Le numéro appelé, l'heure, la durée et le coût de tous les appels téléphoniques externes passés par les terminaux téléphoniques appartenant à la collectivité (fixe & mobile) pendant une durée de 365 jours

La gestion de ces données est faite dans le respect de la loi Informatique et Libertés, qui prévoit, pour toute personne, un droit d'accès et de rectification aux données qui la concernent, ayant fait l'objet d'un traitement informatique. L'exercice de ce droit se fait par la voie hiérarchique.

5.2.2 MESURES CONSERVATOIRES ET SANCTIONS

Tout utilisateur ne suivant pas les règles et obligations rappelées dans cette charte pourra se voir,par mesure conservatoire, suspendre l'accès aux ressources informatiques, téléphoniques, ou à certains services (internet, messagerie…).
En cas de comportement grave et d'intention manifeste de nuire au bon fonctionnement des ressources ou à l'activité des services, il sera passible de sanctions disciplinaires proportionnelles à la gravité des évènements constatés.
Tout utilisateur n'ayant pas respecté les lois pourra être poursuivi civilement et/ou pénalement.

ARTICLE 6 - RGPD

Pour tout traitement de données personnelles, l'agent se conformera au règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, le RGPD.

Si dans l'accomplissement de son travail ou de ses missions, l'utilisateur est amené à mettre en œuvre un traitement des données personnelles (ex. enquêtes, formulaires, etc.), il doit effectuer une déclaration de traitement de données personnelles, informatisé ou non : il devra pour cela contacter le service informatique qui sera chargé de faire le lien auprès du Délégué à la Protection des Données (DPD).
L'agent est informé que les données à caractère personnel le concernant sont conservées au sein du système d'information de la ville de Provins, pendant toute la durée de leur relation contractuelle et des délais en matière de prescription.
L'utilisateur est informé qu'il dispose, pour des motifs légitimes admis par la collectivité, des droits conformes au RGPD tels que droit d'accès, de rectification, d'opposition, droit à l'effacement, à la portabilité, à la limitation du traitement, relatifs à l'ensemble des informations le concernant.
La ville de Provins a désigné un Délégué à la Protection des Données personnelles, le DPO ou DPD.
Le DPO ou DPD a pour mission d'informer, de conseiller et de veiller à la conformité des traitements à la réglementation en matière de données personnelles. Il doit être consulté préalablement à la création d'un traitement (mise en place d'un fichier de données personnelles). Il veille au respect des droits des personnes et peut être sollicité via l'adresse mail suivante : chs.it.consulting@gmail.com

ARTICLE 7 - BASES LEGALES

Le présent article a pour objectif d'informer les utilisateurs des principaux textes législatifs et réglementaires définissant notamment les droits et obligations des personnes utilisant les moyens informatiques. Il ne s'agit en aucune manière d'une liste exhaustive.

- Loi n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires et la loi n°84-53 du26 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale, imposant notamment les obligations de réserve, de discrétion et de secret professionnel des agents publics.
- Loi n°78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.
- Loi n°78-17 du 6 janvier 1978, modifiée, relative à l'informatique, aux fichiers et aux libertés, qui a notamment pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'utilisation de l'informatique et d'encadrer l'utilisation des données à caractère personnel dans les traitements informatiques.
- Loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications.
- Code Pénal, pris notamment en ses articles 323-1 à 323-7 visant les atteintes aux systèmes de traitement automatisé des données.
- Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.
- L'ordonnance N° 2005-1516 du 8 décembre 2005, relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, permet notamment à une administration de répondre par voie électronique à une demande d'information d'un usager ou d'une autre administration qui lui a été adressée par la même voie, et prévoit que les actes des administrations peuvent être signés électroniquement pour assurer l'identification du signataire et l'intégrité des actes.
- Code de la Propriété Intellectuelle. Il reconnaît les logiciels comme œuvres de l'esprit, et à ce titre,ils sont protégés sans nécessiter de dépôt ou d'enregistrement.
- Code du Patrimoine, pris notamment en ses articles L211-1 à L211-4. Il définit les archives comme étant l'ensemble des documents, quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité. Les archives publiques sont notamment les documents qui procèdent de l'activité des collectivités territoriales.
- Loi n°94-665 du 4 août 1994 modifiée, relative à l'emploi de la langue française. Elle prévoit, lorsqu'ils existent, l'emploi de termes français de même sens en lieu et place des termes étrangers...
- Loi no 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, dite loi HADOPI 1 ou loi création et internet
- Le règlement européen pour la protection des données personnelles – RGPD- (UE) n°2016/679 promulgué par la loi d'application n°2018-493 du 20 juin 2018.