
# Charte TIC

Technologies de l'Information et de la Communication

**Charte d'utilisation des systèmes d'information du Conseil général des Hauts-de-Seine.**

**(Usage des ressources informatiques, électroniques, numériques et des réseaux).**

# TABLE DES MATIERES

# LA CHARTE TIC
# DU CONSEIL GENERAL

## 1. POURQUOI UNE CHARTE TIC

- Parce qu'il entend respecter et faire respecter les lois et règlements qui encadrent les activités informatiques,
- Parce qu'il se doit de sauvegarder l'intégrité de son système informatique, son bon fonctionnement et le respect de la confidentialité des données détenues dans ses services,
- Parce qu'il veut organiser la sécurité juridique, eu égard aux éventuels recours liés à des dommages causés par les agents dans l'accomplissement de leurs missions,
- Parce qu'il souhaite promouvoir largement l'usage d'outils informatiques modernes et efficaces sur une base de confiance et de responsabilité partagées,

le Conseil général des Hauts-de-Seine :

- - rappelle à tous les utilisateurs de ses systèmes d'information que certains usages sont pénalement répréhensibles, que d'autres peuvent nuire au bon fonctionnement du réseau ou sont susceptibles d'engager la responsabilité de la collectivité ;
- - fixe par la Charte TIC les règles générales d'utilisation et d'administration des systèmes d'information de la collectivité.

## 2. LA CHARTE TIC

Lors de sa mise en place et de ses premiers développements, l'informatique était centralisée et concernait des services spécialisés dans la saisie et le traitement des données. Les agents de ces petites équipes ont été très tôt sensibilisés aux exigences qui s'attachent à leur domaine : sécurité, fiabilité, confidentialité.

Depuis lors, les systèmes d'information ont considérablement évolué. Dans un premier temps, tous les utilisateurs ont eu accès aux données. Dans un second temps, ils ont participé à leur saisie et à leur traitement. Ces premières étapes répartissaient les tâches. Puis, troisième étape, est venu le temps des échanges d'informations en interne par la messagerie. Aujourd'hui enfin, le développement d'Internet conduit à l'ouverture des systèmes informatiques vers l'extérieur.

Le bon usage de ces nouvelles avancées technologiques nécessite, d'une part, la mise en place de dispositifs techniques adaptés, et, d'autre part, une mise en responsabilité de chaque utilisateur.

Un signe fort de la confiance de notre collectivité à l'égard de chacun de ses agents est de lui donner une adresse Internet personnelle. Aussi est- il est opportun de :

- rappeler les lois et règlements encadrant les activités informatiques,

- officialiser les dispositifs pratiques mis en œuvre par la collectivité pour les faire respecter,
- engager les agents à respecter strictement les règles de bon usage,
- justifier les contrôles opérés par l'administrateur du système informatique.

Le matériel informatique mis à la disposition de l'agent par le Conseil général des Hauts-de-Seine afin qu'il accomplisse sa tâche ne constitue en aucun cas pour lui un espace privé dont l'identifiant qui en protège l'accès serait sa clé personnelle.

Ce dernier a pour seule fonction de protéger l'intégrité des données qu'il contient.

La Charte répond à plusieurs impératifs :

- Sécurité. Nombreux sont les virus et autres comportements hostiles qui peuvent infecter le réseau informatique. Afin d'en assurer le bon fonctionnement, le Conseil général des Hauts-de-Seine organise la protection de son système d'information. Il doit le faire vis à vis des agressions extérieures, mais aussi en proscrivant les usages qui peuvent faciliter l'invasion du réseau.

- Confidentialité. De part ses compétences légales dans plusieurs domaines sensibles, le Conseil général des Hauts-de-Seine a mis en place des serveurs informatiques riches d'informations confidentielles sur les personnes, les entreprises et les institutions. Il serait tenu pour responsable au cas où cette confidentialité n'était pas rigoureusement préservée. Cette obligation de confidentialité nécessite, de la part des utilisateurs, une grande prudence et des usages adaptés.

- Légalité. Certains usages de la messagerie et d'Internet sont pénalement répréhensibles, en particulier, ceux qui portent atteinte au respect des droits d'auteur, la tenue de propos à caractère raciste, la manipulation de documents pédophiles.

- Efficacité. L'usage professionnel de la messagerie et de l'Internet est encouragé afin d'améliorer la qualité, le confort et la rapidité du travail des agents. Un usage privé dans des proportions raisonnables est accepté. L'utilisation abusive de ces outils ne doit cependant pas conduire à une baisse de l'efficacité des services.

La Charte comprend les obligations tant des Utilisateurs que des Administrateurs des systèmes d'information.

Chaque agent sera ainsi informé non seulement des bons usages qui le concernent directement mais aussi des règles qui encadrent l'activité nécessaire de ses collègues chargés du bon fonctionnement du réseau.

Cette forme ramassée et lisible ne peut constituer un document contractuel par son manque d'exhaustivité. Aussi, la Charte constitue un document plus complet avec des annexes et après sa présentation en CTP elle sera mise en ligne sur l'Intranet accompagnée des documents pratiques complémentaires, ainsi que l'ensemble des textes de références. Les liens hypertextes en permettront une consultation efficace.

# 3. L'UTILISATEUR

Toute personne utilisant un poste informatique connecté au réseau de la collectivité est dénommée "utilisateur".

Tout utilisateur est responsable de l'usage des ressources informatiques et du réseau auxquels il a accès, il s'engage à prendre soin des matériels et des installations informatiques mis à sa disposition.

## 3.1 PROPRIETE DU MOT DE PASSE

Chaque utilisateur accède au réseau par un mot de passe personnel, unique et confidentiel, dont il est propriétaire.

A cette signature, sont liées toutes les autorisations d'utilisation de logiciels.

## 3.2 LA RESPONSABILITE DE L'UTILISATEUR

Toutes les connexions réalisées à l'aide du mot de passe de l'utilisateur engagent la responsabilité de son propriétaire.

Le propriétaire doit assurer le secret de sa signature. En cas de doute, il peut à tout moment en changer.

Il lui appartient également d'éteindre ou de verrouiller son poste informatique lorsqu'il quitte son lieu de travail.

## 3.3 LE MATERIEL

L'utilisateur est responsable du matériel qui lui a été confié.

Il ne doit pas modifier sa configuration, ni procéder à des ajouts de périphériques.
Il peut demander par la voie hiérarchique à l'administrateur d'être doté de matériel supplémentaire.

## 3.4 LES LOGICIELS

Chaque utilisateur est doté de logiciels adaptés à ses missions.
Il ne doit pas, sans autorisation, équiper son poste de logiciels supplémentaires.
Il lui est formellement interdit de copier les logiciels d'autres utilisateurs et d'utiliser des logiciels dont la collectivité n'aurait pas acquis les licences.

## 3.5 LES FICHIERS

L'ensemble des données saisies et mises en forme par l'utilisateur dans le cadre de ses missions appartient à la collectivité. Il est pleinement responsable de la sauvegarde de ses productions sous les formes conseillées par l'administrateur.

Tous fichiers de l'utilisateur, hors son dossier « privé » ou « personnel », doivent donc être partagés dans le cadre de l'organisation de la collectivité afin d'assurer la continuité du service public.

La création de fichiers contenant des données personnelles est soumise à autorisation de l'administrateur qui le déclare à la Commission nationale informatique et libertés.

### 3.6 LA MESSAGERIE

La messagerie permet à chaque utilisateur de communiquer en interne et en externe.

En interne, l'utilisateur doit respecter le circuit hiérarchique défini par l'arrêté d'organisation des services, qu'il s'agisse d'interroger, de répondre ou de transférer. Le nombre de copies conformes doit rester limité. La création de copies cachées est déconseillée.

En externe, l'administrateur attribue à chaque utilisateur une adresse personnelle de messagerie. L'utilisateur doit ouvrir sa correspondance électronique et y répondre. Il doit porter une attention particulière à la rédaction de ses messages qui doivent être clairs et écrits en bon français.

Un message peut engager la collectivité. Aussi, l'utilisateur s'assure qu'il a la compétence juridique pour l'adresser. Si tel n'est pas le cas, il transfère le message à sa hiérarchie. L'agent utilise la règle des copies pour informer la hiérarchie. En retour, les messages en copie, permettent à la hiérarchie d'informer l'ensemble des agents concernés. La pratique des copies cachées est proscrite, car elle ne permet pas une circulation transparente de l'information.

L'utilisateur porte une attention particulière à la taille et au contenu des fichiers transmis. Si la taille excède la limite prescrite par l'administrateur, le message est bloqué et éliminé du réseau. Si le contenu a un caractère confidentiel, l'utilisateur doit demander à l'administrateur de lui fournir une solution de cryptage.

Tant en interne qu'en externe, l'utilisateur porte une attention particulière à la rédaction de l'objet. Si le message a un caractère privé, il y fait figurer la mention privé ou personnel et demande à son correspondant externe d'agir de même.

L'envoi en nombre de messages à des utilisateurs qui sont sans rapport avec leur mission et qui ne l'ont pas explicitement souhaité est interdit.

Enfin, aucun message professionnel ou privé ne doit comprendre des éléments de nature offensante, diffamatoire, injurieuse ou à connotation pornographique, sexiste ou raciste.

### 3.7 INTERNET

La navigation sur Internet permet d'accéder et d'échanger rapidement des informations professionnelles. Son usage peut être limité par l'administrateur pour assurer l'intégrité du système et son bon fonctionnement.

L'utilisateur limite son temps de connexion au strict nécessaire. L'accès à des sites connus pour leur caractère strictement commercial doit être exceptionnel.

Il ne participe à aucun forum de discussion, hors accord de sa hiérarchie et, au cas où cette participation engagerait l'image de la collectivité, celui de la direction de la communication.

L'utilisateur peut utiliser le réseau Internet pour garder un lien avec son univers privé. La consultation des sites à titre privé est autorisée dans la mesure où le temps de navigation ne gêne pas de façon significative l'exercice de ses missions et sa disponibilité.
Sont interdits, sauf dérogation expresse de l'administrateur accordées au regard des missions de l'utilisateur, les actes commerciaux d'achat ainsi que les téléchargements de logiciels ou d'autres œuvres protégées (livre, musique, photo, vidéo).

La consultation et le téléchargement du contenu de sites à caractère pornographique sont interdites. L'accès à certains sites illégaux (pédophiles par exemple) peut même revêtir le caractère d'une infraction pénale. Cette activité est strictement interdite. L'Administrateur se réserve le droit de dénoncer tout acte délictueux aux autorités, et ce, sans préjudice de l'application des sanctions administratives prévues à l'article 6 de la Charte.

### 3.8 DOSSIER PERSONNEL INFORMATIQUE

L'utilisation privée de la messagerie et d'Internet n'est pas interdite, mais limitée (Cf. 6 et 7).
L'ensemble des données que l'utilisateur souhaite garder confidentielles et dont il assume la pleine et entière responsabilité doit être rassemblée dans un dossier personnel unique et clairement identifié.

### 3.9 OBLIGATION DE VIGILANCE

Chaque utilisateur contribue, à son niveau, à la sécurité du système informatique.
Tout dysfonctionnement ou anomalie constatée par l'utilisateur, toute erreur d'utilisation pouvant entraîner des conséquences dommageables, doit être signalé, sans retard, à l'administrateur.

# 4. LES UTILISATEURS COLLECTIFS

Les utilisateurs collectifs du Conseil général des Hauts-de-Seine ont accès aux systèmes d'information du Conseil général sous réserve du respect de l'intégralité des dispositions de la présente Charte, à condition qu'ils en soient signataires.

Par dérogation, les syndicats représentatifs au sein de la collectivité ont accès aux ressources informatiques du Conseil général qu'ils en soient ou non signataires sous réserve d'en respecter l'intégralité des dispositions

## 4.1 PROPRIETE

Les moyens matériels et logiciels mis à la disposition des utilisateurs collectifs demeurent la propriété du Conseil général des Hauts-de-Seine.

## 4.2 CONFIDENTIALITE DES ECHANGES

Le Conseil général des Hauts-de-Seine s'engage à respecter la confidentialité des messages électroniques en provenance ou à destination des boîtes aux lettres des utilisateurs collectifs. Il ne peut pour autant être tenu pour responsable des violations qui pourraient être commises par des tiers.

## 4.3 RESPONSABILITE DES UTILISATEURS COLLECTIFS ET DE LEURS MEMBRES

Les utilisateurs collectifs ainsi que leurs membres engagent leur responsabilité sur le contenu et la gestion des ressources mises à leur disposition. Ils en assument ainsi l'entière responsabilité éditoriale et technique.

C'est en particulier le cas dans l'hypothèse du non-respect des dispositions légales et réglementaires, notamment en matière pénale (par exemple, injure et diffamation, contrefaçon, obligations résultant de la loi informatique et libertés, etc.) ou statutaires (par exemple, violation du devoir de discrétion professionnelle ou de l'obligation de réserve).

Chaque utilisateur collectif ainsi que ses membres devront répondre personnellement, notamment, de la gestion, la conservation, la sauvegarde, la protection ou encore de la déclaration à la CNIL des fichiers dont ils ont l'usage, la détention ou qu'ils constituent, à quelque titre que ce soit.

## 4.4 MESSAGERIE INTERNE

II est attribué des boîtes aux lettres aux coordonnées des utilisateurs collectifs destinées aux messages relevant de leur activité collective qui seules doivent servir à l'envoi de messages en relevant, à l'exclusion des boîtes qui sont attribuées à chacun dans le cadre professionnel.

Il est expressément indiqué, dans le cadre de l'utilisation des ressources et particulièrement de la messagerie que l'interactivité, le « streaming », la diffusion de textes ou documents de diffusion générale par messagerie, le « spamming », la répercussion en « chaîne » de

messages non professionnels, les forums, le « chat », les « applets » Java, les moteurs de recherche et les « cookies » ne sont pas autorisés.

Les envois généraux aux agents ne sont donc pas autorisés et seuls sont admis les messages à destination de ceux qui ont préalablement manifesté la volonté d'en être destinataires en s'inscrivant sur une liste de diffusion ; l'envoi de tels messages devra être arrêté dès que l'Intéressé le demandera à l'émetteur ou à ceux dont la fonction est de transmettre l'information.

Par l'Intranet du Conseil général des Hauts-de-Seine, les utilisateurs collectifs pourront renvoyer leurs interlocuteurs vers leur site web externe par des liens hypertextes ou autres.

# 5. L'ADMINISTRATEUR

Le responsable des systèmes d'information, dénommé "administrateur", assure la direction de toutes les activités liées à la production, au transport et au stockage des données informatiques (Direction des systèmes d'information du Conseil général des Hauts-de-Seine)

Il a accès à toutes les données qui s'échangent tant sur le réseau interne qu'avec l'extérieur.

Il est tenu à un strict respect du secret professionnel.

## 5.1 FONCTIONNEMENT DU SYSTEME

L'administrateur est responsable du bon fonctionnement du système informatique.

Il dimensionne les installations et les réseaux aussi bien que les volumes des fichiers transmis et les durées de connexions.

Il alloue à chaque utilisateur les ressources nécessaires à l'exercice de ses fonctions.

## 5.2 DEVOIR DE PROTECTION

L'administrateur est responsable de l'intégrité du système.

Il met en place les outils nécessaires à protéger les réseaux de toute intrusion, pollution ou acte hostile.

## 5.3 NECESSITE DE SURVEILLANCE

A la fois pour assurer un bon fonctionnement et une protection du réseau, l'administrateur doit veiller au bon usage des ressources par les utilisateurs.

## 5.4 CONTROLE SYSTEMATIQUE

L'administrateur contrôle que les matériels et logiciels des utilisateurs sont conformes aux besoins définis par leur hiérarchie. Concernant leur usage, il comptabilise les temps de connexions, les sites visités, les volumes téléchargés ainsi que toutes activités relatives à l'usage des micro-ordinateurs et serveurs, de la messagerie électronique, d'Intranet et d'Internet. Il réalise des rapports périodiques non personnalisés, transmissibles par voie hiérarchique.

En cas de détection de comportements non conformes à la Charte, l'administrateur peut, après en avoir informé personnellement et par écrit l'utilisateur, réaliser une surveillance personnelle dont les résultats sont communiqués à l'autorité territoriale.

Dans tous les cas l'Administrateur se garde le droit d'effacer, de comprimer ou d'isoler toute donnée ou fichier manifestement en contradiction avec la Charte ou qui mettrait en péril la sécurité des moyens informatiques,

### 5.5 ANALYSE ET CONTROLE DE L'UTILISATION DES RESSOURCES

Pour des nécessités de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau informatique sont analysés et contrôlés dans le respect de la législation applicable et notamment de la loi sur l'informatique et les libertés.

Par ailleurs, dans le cadre de sa mission de protection des systèmes d'information, d'engagement de sa responsabilité et de l'amélioration de sa productivité, le Conseil général enregistre les durées des connexions, les sites les plus visités et les volumes téléchargés ainsi que toutes activités relatives à l'usage des micro-ordinateurs et serveurs, de la messagerie électronique, d'Intranet et d'Internet.

En particulier, un rapport trimestriel non nominatif des sites les plus visités peut être remis à la Direction générale des services.

Le Conseil général se réserve le droit de suspendre à tout moment, et sans avertissement, l'accès aux systèmes d'information (sites Internet notamment), en cas d'inobservation des présentes règles par l'utilisateur.

Le Conseil général se réserve en outre le droit de bloquer à tout moment, sans avertissement préalable, l'accès aux sites dont le contenu est jugé illégal ou offensant.

### 5.6 RESPECT DE LA VIE PRIVEE

L'administrateur est tenu à un strict respect du secret professionnel.
La surveillance de l'administrateur ne s'exerce pas sur les dossiers informatiques « privés » ou « personnels ».

### 5.7 RESPECT DE LA LEGALITE DES USAGES DES OUTILS TIC

Sans préjudice de la confidentialité des correspondances, l'administrateur est tenu de dénoncer au Procureur de la République les usages illégaux (tels que pédophilie, incitation à la haine raciale, terrorisme) qu'il constaterait dans l'usage des outils T.I.C.

# 6. LA PORTEE DE LA CHARTE

## 6.1 QUI EST CONCERNE PAR LA CHARTE ?

La Charte s'applique à **toute personne ayant accès aux systèmes d'information du Conseil général des Hauts-de-Seine,** entre autres et de façon non exhaustive : les agents titulaires, contractuels ou stagiaires, quels que soient leur fonction, leur grade ou leur service, les vacataires et les prestataires.

## 6.2 NATURE DE LA CHARTE

Elle remplace et annule toutes dispositions contraires contenues dans les notes de service et autres réglementations existantes en vigueur relatives au fonctionnement et l'utilisation des systèmes d'information du Conseil général des Hauts-de-Seine, qu'elles soient écrites ou orales.

## 6.3 MODALITES D'APPLICATION

La Charte est applicable dès sa promulgation officielle, après examen par le Comité Technique Paritaire.

Elle est présentée à l'agent fonctionnaire au moment de sa prise de fonction, de même qu'aux agents contractuels ou vacataires.

Elle sera communiquée aux fournisseurs titulaires de marchés dont les salariés ou sous-traitants sont amenés, dans le cadre de leur prestation, à avoir accès aux systèmes informatiques du Conseil général des Hauts-de-Seine. A charge pour eux de la communiquer aux personnes intervenant de leur fait.

La Charte d'utilisation et, toutes les explications techniques nécessaires à sa bonne compréhension, constitueront des rubriques permanentes présentes sur l'Intranet du Conseil général des Hauts-de-Seine.

## 6.4 EVOLUTION DE LA CHARTE

La présente Charte TIC établie dans l'intérêt des utilisateurs du Conseil général des Hauts-de-Seine, qui de ce fait sont informés et acceptent, les risques inhérents à l'utilisation des systèmes d'information. Elle a été soumise pour avis au CTP du 23 juin 2005 et entrera en application le 1er juillet 2005.

Cette Charte pourra être complétée par des consignes de « bons usages » des systèmes d'information, sous forme de « note de service »

Chaque utilisateur de la Charte est invité à transmettre à la Direction des systèmes d'information les propositions d'amendements dont il a pu constater l'intérêt dans le cadre de sa pratique personnelle des ressources des systèmes d'information. Ces suggestions seront prises en compte dans le cadre des concertations préalables aux mises à jour ultérieures de la Charte.


# Charte TIC

## ANNEXE TECHNIQUE
## Conseils à l'intention
## des utilisateurs des systèmes d'information

# ANNEXE TECHNIQUE

# CONSEILS A L'INTENTION DES UTILISATEURS DES SYSTEMES D'INFORMATION

## 1 INTRODUCTION

Elaborée en collaboration étroite avec les représentants des organisations syndicales du Conseil général des Hauts-de-Seine et présentée au CTP du 23 juin 2005, en cohérence totale avec la « CHARTE TIC » du Conseil général.

Le présent document précise les bons usages et les attitudes souhaitées vis à vis de ses collègues, fournisseurs, interlocuteurs ainsi que de la collectivité. Il complète la « CHARTE TIC » sur des questions d'ordre technique. Le non respect des consignes du présent document n'est pas soumis aux règles disciplinaires.

Il est mis à jour par la Direction des systèmes d'information en fonction des besoins des utilisateurs et des évolutions technologiques des systèmes d'information du Conseil général des Hauts-de-Seine.

## 2 LES SYSTEMES D'INFORMATION

On entend par systèmes d'information du Conseil général des Hauts-de-Seine :

- l'ensemble des ordinateurs, fixes ou portables, et tout autre matériel informatique, connectique ou bureautique y compris les serveurs, hubs, câbles du réseau, (" Matériel ") ;

- l'ensemble des logiciels contenus dans ou faisant fonctionner, interopérer ou protégeant lesdits ordinateurs et matériels informatiques, y compris les protocoles de communication TCP/IP, (" Logiciel ")

  **permettant :**
  - la constitution et la création
  - l'échange, la circulation, la diffusion,
  - la duplication, reproduction et stockage, (" Opérations ")

  **de :**
  - données, fichiers, base de données,
  - intranet, extranet
  - images, sons, textes,
  - flux quelconques d'information, (" Informations ")

  **entre :**
  - les " Utilisateurs " entre eux,
  - les " Utilisateurs " et l'extérieur,

  et ce quelle que soit la finalité du flux d'information.

- l'ensemble des données sauvegardées sur les serveurs du Conseil général des Hauts-de-Seine ou sur les postes individuels.

## 3 PRINCIPES DE BASE

Les principes de base sur lesquels ont été élaborées ces règles des bons usages et des bonnes pratiques sont :

- Amélioration des conditions de travail par une ouverture à l'Internet et à la messagerie électronique pour élever le niveau des compétences et augmenter l'efficacité du Conseil général des Hauts-de-Seine.

- Transparence et courtoisie. L'Utilisateur s'engage donc à transmettre autant que faire se peut ses coordonnées professionnelles personnalisées, à répondre rapidement et à être discret sur l'ensemble des informations personnelles, professionnelles ou techniques qu'il peut détenir.

- Pas de modification ou d'ajout de matériel sans l'accord écrit de l'Administrateur. Le matériel mis à la disposition des Utilisateurs a été défini en relation avec les directions métiers. Il est donc adapté à la tâche.

- Pas de modification ou d'ajout de logiciels sans l'accord écrit de l'Administrateur. Les logiciels mis à disposition ont été choisis en relation avec les directions métiers. Ils sont donc adapté. Plus particulièrement, aucun logiciel ou autre programme ne doit être téléchargé et installé sans l'accord écrit de l'Administrateur.

- Pas d'encombrement inutile du réseau et des serveurs. L'Utilisateur veillera donc au volume des fichiers qu'il transmet et sauvegarde.

## 4 CONCERNANT LA SECURITE DU SYSTEME D'INFORMATION

### La protection des systèmes d'information c'est :

- la conservation et la sauvegarde des données,
- la surveillance contre la diffusion non autorisée des informations techniques, administratives et autres informations appartenant à l'administration,
- la preuve de la date de création ou de la diffusion desdites informations,
- la protection de l'intégrité des données et du fonctionnement des systèmes d'information,
- la protection contre l'intrusion dans les systèmes d'information,
- la surveillance contre l'intrusion ou l'utilisation de matériels violant les règles relatives au droit d'auteur, copyright, par exemple pour défaut de licence d'utilisation,
- le bon fonctionnement du matériel et des installations mises à disposition,
- la mise à jour, maintenance, correction, réparation des « Matériels » et « Logiciels ».

### L'Utilisateur :

- doit appliquer les recommandations de sécurité du service auquel il appartient,
- doit assurer la protection de ses informations, en particulier, il est responsable des droits qu'il donne aux autres utilisateurs,
- il lui appartient de protéger ses données professionnelles en les stockant sur les unités serveurs mises à sa disposition,
- doit veiller à ne stocker que la dernière version des documents utiles sur les serveurs bureautiques et à supprimer régulièrement les documents qui ne servent plus,
- doit signaler toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater,
- s'engage à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux, à travers des matériels dont il a l'usage,
- ne doit pas utiliser ou essayer d'utiliser des comptes autres que le sien ou masquer sa véritable identité,
- ne doit pas tenter de lire, modifier, copier ou détruire des données autres que celles qui lui appartiennent en propre, directement ou indirectement,
- d'envoyer et/ou, en cas de réception, d'ouvrir des fichiers "exécutables" (terminaison en .exe), en raison de la menace sérieuse qu'ils constituent pour la stabilité et la sécurité du réseau de la collectivité (virus, etc...),
- ne doit pas quitter son poste de travail ni ceux en libre-service sans le verrouiller ou sans se déconnecter en laissant des ressources ou services accessibles.

## 5 CONCERNANT LE POSTE DE TRAVAIL ET LA RESPONSABILITE PERSONNELLE

Les bonnes pratiques de respect de la confidentialité et de la meilleure sécurité :

- Le code d'accès (mot de passe) est confidentiel et devra être modifié selon une fréquence que l'utilisateur jugera opportune ou sur préconisation de l'Administrateur.
- En aucune manière ils ne doivent être notés sur son ordinateur ou un matériel qui y est rattaché. L'Utilisateur doit le mémoriser.
- En cas d'oubli, seul l'Administrateur du réseau pourra communiquer de nouveau le mot de passe à l'Utilisateur.
- Si, les circonstances l'exigeant, il doit communiquer son mot de passe aux équipes techniques de maintenance, il est de la responsabilité de l'Utilisateur de le changer après l'intervention.
- Concernant les interventions (à distance ou en local) d'un prestataire de service informatique extérieur au Conseil général, l'utilisateur s'engage à ne pas laisser son poste de travail en mode connectable une fois l'intervention terminée.
- Concernant les connexions par modem, l'utilisateur s'engage à ne pas rester connecté au-delà du temps strictement nécessaire à la réalisation de ses obligations professionnelles.
- Ce droit d'accès disparaît automatiquement dès lors que son titulaire quitte, de manière temporaire ou définitive, le Conseil général.
- L'Utilisateur s'empêchera toute connexion non autorisée de matériel par les prises d'accès « à chaud » disponibles : clef USB, Firewire, …

## 6 CONCERNANT LE CAS DES FICHIERS EN PARTAGE RESERVE

L'utilisation des ressources informatiques partagées du Conseil général et la connexion d'un équipement sur le réseau sont soumises à autorisation.

- Un mot de passe spécifique peut être donné à l'Utilisateur pour accéder ou faire fonctionner la messagerie électronique, ou pour accéder à des fichiers en partage réservé.

- Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Ces autorisations peuvent être retirées à tout moment.

- Toute autorisation prend fin lors de la cessation même provisoire de l'activité professionnelle qui l'a justifiée.

## 7 CONCERNANT LES USAGES DE LA MESSAGERIE ELECTRONIQUE

La règle des messages en copie reprend exactement celle du courrier écrit traditionnel :

- Destinataire principal : la (les) personne(s) concernée(s) directement par le message,
- Copie conforme (CC) : son propre supérieur hiérarchique et toute personne concernée par son contenu,
- Pas de copie cachée (CCI).

Quand une réponse engage le Conseil général des Hauts-de-Seine sur le plan moral ou financier, quand cette réponse n'est pas signée par la personne ayant délégation car elle est émise d'un autre poste informatique (celui de la secrétaire par exemple), le message doit obligatoirement mentionné que l'engagement est exprimé au nom, lieu et place du délégataire de la signature.

Le logiciel de messagerie (Microsoft Outlook) propose une fonction de calendrier. Celle-ci, couplée à l'annuaire, permet de gérer les agendas et d'organiser rapidement des réunions de travail.

L'Utilisateur s'attachera donc à garder à jour son Agenda électronique.

## 8 CONCERNANT LA CIRCULATION DES FICHIERS

Le volume des fichiers échangés circulant sur le réseau interne du Conseil général des Hauts-de-Seine n'est pas limité. Par contre, dans le cas de fichiers envoyés ou reçus de l'extérieur, l'Administrateur a limité à 10 Mo[1] la taille des messages électroniques y compris les pièces jointes les accompagnant. Il est interdit d'envoyer des messages ne respectant pas la taille prescrite par l'Administrateur : ils seront automatiquement bloqués par le Firewall et éliminés du réseau. L'Utilisateur sera alors informé par l'Administrateur de la non distribution de son message.

Dans le cas où l'échange de gros fichiers est nécessaire, on demandera à l'Administrateur un accès au serveur FTP réservé à cet usage.

## 9 LES BOITES AUX LETTRES NOMINATIVES

Il existe un domaine propre au Conseil général « cg92.fr ».

Les boîtes aux lettres nominatives sont toutes construites sur le même modèle :
*«première lettre du prénom en minuscule suivi du nom en minuscule @cg92.fr »*
ex : (*jmartin@cg92.fr*).

[1] Paramètre susceptible d'évoluer en fonction des capacités techniques des systèmes.


# Charte TIC

## ANNEXE JURIDIQUE
## LES TEXTES DE REFERENCE

# ANNEXE JURIDIQUE
# LES TEXTES DE REFERENCE

## 1. CADRE LEGISLATIF

Les lois principales encadrant cette Charte sont celles régissant :

- La responsabilité du Conseil général des Hauts-de-Seine
- La protection de la vie privée des agents
- Les règles de la transparence et de la concertation
- Les règles générales de respect mutuel
- La protection des personnes inscrites dans les bases de données du Conseil général des Hauts-de-Seine
- La protection de l'intégrité technique des systèmes d'information du Conseil général des Hauts-de-Seine

## 2. TRANSPARENCE ET CONCERTATION

- **Le décret de 1982** régit les obligations de consulter le CTP
- **L'article L 432-2-2 du code du travail** prévoit la consultation obligatoire du CTP lorsque l'employeur projette d'introduire dans l'entreprise des moyens qui rendent possible la surveillance des salariés.
- **L'article L 412-8 du code du travail** modifié par l'article 45 de la loi relative à la formation professionnelle tout au long de la vie et au dialogue social, adoptée le 7 avril 2004. La nouvelle rédaction de cet article ne procure aucun droit nouveau en matière de communication syndicale sur les outils électroniques de l'entreprise.

## 3 RESPONSABILITE DU CONSEIL GENERAL DES HAUTS-DE-SEINE

- **L'article 1384 alinéa 5 du Code Civil** prévoit la responsabilité civile de l'employeur du dommage causé par ses préposés dans les fonctions auxquelles il les a employés.
- **Code du Travail, article L120-2 :** "Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché"
- **L'article L.121 - 8 du code de travail** (directement issu de la loi du 6/1/78 dite "informatique et liberté") aux termes duquel "aucune information concernant personnellement un salarié ou un candidat à un emploi ne peut être collecté par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié ou du candidat à un emploi."

## 4 PROTECTION DE LA VIE PRIVEE DES AGENTS

- **L'article 9 du Code Civil,**
- **l'article 8 de la Convention européenne de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales et**
- **l'article 226-1 du Code Pénal sur la protection du courrier privé et, par extension, du courrier électronique.**
- **La loi numéro 91-646 du 10 juillet 1991 article 2** stipule: "Le secret des correspondances émises par la voie des télécommunications est garanti par la loi".
- **L'articles 226-15 et 432-9 du nouveau code pénal** fixe de lourdes sanctions pénales pour celui qui porte atteinte au secret de la correspondance. Les utilisateurs doivent s'abstenir de toute tentative d'intercepter les communications privées, qu'il s'agisse de courrier électronique ou de dialogue direct

## 5 REGLES GENERALES DE RESPECT DES DROITS D'AUTRUI

- **Les lois numéro 90-615 du 13 juillet 1990 et numéro 92-1336 du 16 décembre 1992** interdisent de faire l'apologie du racisme, de l'antisémitisme et de la xénophobie.
- La législation relative à la propriété intellectuelle.
- **Loi du 29 juillet 1881** sur la Liberté de la presse qui réglemente la nature des contenus
- **Interdiction de** proférer menace ou injure à l'égard des personnes.

## 6 ENREGISTREMENT DE DONNEES NOMINATIVES ET REGLES ISSUES DE LA LOI « INFORMATIQUE ET LIBERTES »

- **L'articles 226-16 à 226-22 du nouveau code pénal** sur « les atteintes aux droits des personnes résultant des fichiers ou des traitements informatique » définit qu'il y a délits non pas seulement s'il y a intention coupable mais dès lors qu'il y a négligence, imprudence ou même incompétence professionnelle ;

- Les actes enfreignant les systèmes automatisés de traitement des données personnelles **(articles 323-1 à 323-7 du code pénal)**

- Il est rappelé qu'en cas d'atteinte à l'un des principes protégés par la loi, la responsabilité pénale ou civile de l'agent ainsi que celle de la collectivité est susceptible d'être recherchée. **(410-1, 411-6 et 432-9 al.1 du Nouveau Code Pénal).**

**Textes en vigueur (loi « Informatique et Libertés »)**

**Article 226-16** Le fait (L. n° 92-1336 du 16 déc. 1992) ", y compris par négligence," de procéder ou de faire procéder à des traitements automatisés d'informations nominatives sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de trois ans d'emprisonnement et de 300 000 F d'amende.

**Article 226-17** Le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés est puni de cinq ans d'emprisonnement et de 2 000 000 F d'amende.

**Article 226-18** Le fait de collecter des données par un moyen frauduleux, déloyal ou illicite, ou de procéder à un traitement d'informations nominatives concernant une personne physique malgré l'opposition de cette personne, lorsque cette opposition est fondée sur des raisons légitimes, est puni de cinq ans d'emprisonnement et de 2 000 000 F d'amende. (Loi n° 94-548 du 1er juillet 1994, art. 4.) "

En cas de traitement automatise de données nominatives ayant pour fin la recherche dans le domaine de la santé, est puni des mêmes peines le fait de procéder à un traitement: "1° Sans avoir préalablement informé individuellement les personnes sur le compte desquelles des données nominatives sont recueillies ou transmises de leur droit d'accès, de rectification et d'opposition, de la nature des informations transmises et des destinataires des données; "2° Malgré l'opposition de la personne concernée ou, lorsqu'il est prévu par la loi, en l'absence du consentement éclairé et exprès de la personne, ou, s'il s'agit d'une personne décédée, malgré le refus exprimé par celle-ci de son vivant. "

**Article 226-19** Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans l'accord exprès de l'intéressé, des données nominatives qui, directement ou indirectement, font apparaître les origines raciales ou les opinions

politiques, philosophiques ou religieuses ou les appartenances syndicales ou les moeurs des personnes est puni de cinq ans d'emprisonnement et de 2 000 000 F d'amende. Est puni des mêmes peines le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée des informations nominatives concernant des infractions, des condamnations ou des mesures de sûreté.

**Article 226-20** (Modifié par la loi n° 2000-321 du 12 avril 2000, article 6)
I - Le fait de conserver des informations sous une forme nominative au-delà de la durée prévue par la demande d'avis ou la déclaration préalable, la mise en oeuvre du traitement informatisé est puni de trois ans d'emprisonnement et de 300 000 F d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi.
II - Le fait de traiter des informations nominatives conservées au-delà de la durée mentionnée au I à des fins autres qu'historiques, statistiques ou scientifiques est puni des mêmes peines, sauf si ce traitement a été autorisé dans les conditions prévues par la loi.

**Article 226-21** Le fait, par toute personne détentrice d'informations nominatives à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative ou l'acte réglementaire autorisant le traitement automatise, (Loi n° 95-116 du 4 février 1995, art. 34) "ou par la décision de la Commission nationale de l'informatique et des libertés autorisant un traitement automatisé ayant pour fin la recherche dans le domaine de la santé," ou par les déclarations préalables à la mise en oeuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 2 000 000 F d'amende.

**Article 226-22** Le fait, par toute personne qui a recueilli à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des informations nominatives dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou a l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces informations à la connaissance d'un tiers qui n'a pas qualité pour les recevoir, est puni d'un an d'emprisonnement et de 100 000 F d'amende. La divulgation prévue à l'alinéa précédent est punie de 50 000 F d'amende lorsqu'elle a été commise par imprudence ou négligence. Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit.

**Article 226-23** Les dispositions des articles 226-17 à 226-19 sont applicables aux fichiers non automatisés ou mécanographiques dont l'usage ne relève pas exclusivement de l'exercice du droit à la vie privée.

**Article 226-24** Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies aux articles 226-16 à 226-21 et 226-23 ainsi qu'au premier alinéa de l'article 226-22. Les peines encourues par les personnes morales sont: 1° L'amende, suivant les modalités prévues par l'article 131-38; 2° Les peines mentionnées aux 2°, 3°, 4°, 5°, 7°, 8° et 9° de l'article 131-39. L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

## 7 DES RESPONSABILITES PENALES EN CAS D'ATTEINTE AUX SYSTEMES DE TRAITEMENT AUTOMATISE DE DONNEES

- **L'article 323-1 du nouveau code pénal** stipule que la simple accession à un système sans autorisation constitue un délit, même s'il n'en est résulté aucune altération des données ou fonctionnement dudit système. Si de telles altérations sont constatées les sanctions prévues sont doublées.

- **L'article 323-2 du nouveau code pénal** concerne les actes consistant à empêcher un système de fonctionner par exemple par l'introduction de "virus".

- Les **articles 323-3 et 323-4** du nouveau code pénal concernent l'introduction ou la modification frauduleuse de données.

- **L'article 323-5 du nouveau code pénal** stipule que de tels actes (même de simples tentatives) sont susceptibles d'entraîner l'éviction de la fonction publique.

- Les actes enfreignant les droits et obligations des personnes utilisant les moyens informatiques **(article 226-15 al.1 à 226-24 du code pénal** (atteintes aux droits des personnes),

**Textes en vigueur (chap. III du Code Pénal)**

**Article 323-1** Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 100 000 F d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 200 000 F d'amende.

**Article 323-2** Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 300 000 F d'amende.

**Article 323-3** Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de trois ans d'emprisonnement et de 300 000 F d'amende.

**Article 323-4** La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

**Article 323-5** Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :
1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;
2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de

laquelle l'infraction a été commise ;
3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;
4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;
6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;
7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35.

**Article 323-6** Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre.
Les peines encourues par les personnes morales sont :
1° L'amende, suivant les modalités prévues par l'article 131-38 ;
2° Les peines mentionnées à l'article 131-39.
L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

**Article 323-7** La tentative des délits prévus par les articles 323-1 à 323-3 est punie des mêmes peines.