DEPARTEMENT DE LA GIRONDE

# CHARTE DE BON USAGE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

DEPARTEMENT DE LA GIRONDE

2016

Cette charte a pour but d'établir un code de déontologie pour régir l'utilisation des ressources informatiques mises à la disposition des utilisateurs. Elle sert également à faire prendre conscience aux utilisateurs de certains risques qu'ils pourraient encourir et des conséquences de tels risques pour le Département de la Gironde.

# Préambule

**Pourquoi une Charte de bon usage des technologies de l'information et de la communication ?**

Le Département de la Gironde est exposé à des responsabilités importantes dans le cadre de ses activités, des actions de ses agents et notamment vis-à-vis des moyens qui leur sont affectés dans le cadre de leur activité professionnelle.

Le « bon usage » des ressources des technologies de l'information et de la communication (TIC) du Département s'entend d'un usage responsable : il fait appel au bon sens, à l'attention et à la prudence.

Il s'appuie sur des prescriptions, des conseils et des recommandations techniques ou d'usage. Le bon usage se réfère également à des règles de déontologie professionnelle et de déontologie personnelle : chacun doit clairement prendre conscience de ce à quoi il s'engage.

L'usage des TIC doit aussi respecter un cadre légal. Toute personne, dans le cadre de son activité professionnelle, eut, outre sa responsabilité professionnelle, voir engagées ses responsabilités personnelle, civile ou pénale,

Si la Charte rappelle de grands principes et des règles de fonctionnement qui sont portés à la connaissance de tous, elle vise aussi à informer les utilisateurs de leurs devoirs et de leurs droits, notamment en ce qui concerne la confidentialité et le respect de la vie privée.

Le respect de cette Charte permettra de sécuriser au quotidien le Conseil Général de la Gironde et ses utilisateurs contre les risques exposés par l'utilisation des TIC.

L'objectif de cette charte n'est pas de restreindre l'usage de ces TIC, mais de définir un cadre d'utilisation, qui soit contrôlable, en accord avec la réglementation.

Cette charte est portée à la connaissance et s'impose à tous.

**LE DEVOIR DE CONFIDENTIALITÉ EST GÉNÉRAL ET PERMANENT**

# Champ d'application de la charte

**Les utilisateurs**

Cette charte s'applique aux personnes ayant un accès au Système d'Information du Département de la Gironde :

- Agents du Département
- Elus du Département,
- Invités (partenaires, prestataires, stagiaires, sous-traitants) : toute personne ayant été dûment autorisée à utiliser une ressource informatique du Département. Les obligations de l'invité dans le cadre de l'usage de ressources informatiques sont identiques à celles d'un agent.

**Les ressources et les données**

La charte s'applique à l'ensemble des ressources informatiques et des moyens de communication électronique du Département :

- Postes de travail (PC, ordinateurs portables, appareils mobiles, tablettes...), périphériques d'impression et de stockage externes, logiciels bureautiques et métiers ;
- Messageries électroniques et accès à Internet, à l'Intranet et l'Extranet;
- Réseau informatique et de télécommunication, serveurs, systèmes de sécurité et de collecte des données ;
- Téléphonie (téléphones fixes et mobiles, smartphones, PDA, fax...)
- Système d'information au sens large, dont logiciels, applications métiers, données (numériques, images, sons) et échanges de fichiers.

Les utilisateurs ont des droits gérés au niveau de la Direction des Systèmes d'Information (DSI) du Département de la Gironde (accès aux ressources confidentielles) mais ils ont également des devoirs. L'ensemble de ces droits et devoirs est développé à partir du chapitre « conditions d'accès ».

**Droits et devoirs de la DSI**

Les agents ou invités de la DSI sont garants de l'application rigoureuse des recommandations de cette charte. Ces personnes ont des droits qui leur sont indispensables pour le bon fonctionnement du réseau interne mais sont bien sûr également soumises à la loi française.

La DSI se doit de fournir à chaque utilisateur :

- un accès physique au réseau lié à son adresse professionnelle dans la limite des moyens humains et matériels disponibles et dans la mesure où l'utilisateur respecte la charte.
- le respect de la confidentialité.

La DSI se réserve le droit, selon les modalités décrites aux chapitres 4 et 5, de :

- vérifier que les activités en cours sur le système d'information respectent la charte (étude des journaux de bord, des traces applicatives et systèmes...) en accord avec les termes de la loi Informatique et Liberté du 6 Janvier 1978.
- prendre les dispositions nécessaires à l'encontre d'un utilisateur ou d'un matériel informatique qui gênerait le bon fonctionnement des ressources informatiques

# Conditions d'accès

**Les demandes d'accès et d'équipement**

Toutes les demandes d'accès au système d'information, de dotation d'équipement, de logiciels, d'accès aux applications pour les métiers sont soumises à validation via le processus de demande mis en place par la DSI (« catalogue des services DSI») accessible depuis l'intranet Mascaret.

Chaque ressource mise à disposition d'un utilisateur lui est affectée nominativement pour la durée de sa mission, au sein d'une direction, d'un service, d'un métier et d'une fonction précise.

Toute modification de ce contexte de travail (mobilité, départ...), ayant un impact sur l'utilisation du SI, doit être signalée à la DSI et aux administrateurs fonctionnels concernés pour actualisation des droits d'accès.

En ce qui concerne les matériels dit « libre-service » ou « en pool », ils sont systématiquement affectés au responsable hiérarchique de la structure.

**Les codes d'accès personnels**

Chaque utilisateur accède aux différentes ressources par un identifiant personnel composé d'un compte utilisateur (ou login) et d'un mot de passe.

Le compte utilisateur et son mot de passe sont strictement individuels et confidentiels. Ils ne doivent jamais être transmis, cédés ou être mise en évidence et facilement accessible par d'autres personnes.

L'utilisateur est responsable du maintien de la confidentialité de ses codes d'accès.

Il lui appartient de modifier périodiquement ses mots de passe en respectant un niveau de robustesse minimum (chiffres, lettres, majuscules, minuscules en accord avec la politique de sécurité du Département de la Gironde).

Il veille à verrouiller sa session de travail Windows lorsqu'il s'absente, même pendant une courte durée.

Sont interdites les actions intentionnelles visant à :

- accéder frauduleusement à un ordinateur,
- usurper des comptes et mots de passe,
- masquer sa véritable identité,
- désactiver les systèmes de protection (antivirus, pare-feu, etc.),
- accéder à des supports externes (disque dur externe, cd-rom, clé USB) sans le consentement explicite de leur propriétaire.
- contourner tous types de mécanismes de sécurité mis en place par la DSI

**L'authentification forte**

Pour certaines applications sensibles, des dispositions d'authentification forte ont été délivrées. L'usage de ces dispositifs (cartes à puce et certificats électroniques) est personnel et ne doit en aucun cas faire l'objet d'une cession quelle que soit sa nature (prêt, délégation…).

**Départ d'un utilisateur**

Lors du départ d'un utilisateur de la collectivité, ce dernier doit restituer les moyens informatiques et de communication électronique qui lui ont été confiés. Son répertoire « personnel » s'il n'a pas été détruit par ce dernier, sera supprimé sans réalisation de copie, ni prise de connaissance préalable du contenu par la Collectivité. Les comptes et droits d'accès associés seront fermés.

# Conditions d'utilisation

L'utilisation des ressources (postes de travail, téléphone, internet, messagerie...) mises à disposition est destinée à un usage professionnel. Un usage personnel raisonnable est toutefois admis et reste sous l'entière responsabilité de l'utilisateur.

Les composants techniques mis à disposition de l'utilisateur pour ses activités professionnelles font l'objet, par le Département, de mesures techniques de sécurité.

Tout dysfonctionnement doit être signalé à la DSI qui est seule habilitée pour décider des actions à entreprendre. Par dérogation validée par la DSI, certaines actions pourront être effectuées par les administrateurs fonctionnels, ou les correspondants informatiques.

**Règles à respecter pour les postes de travail**

Les seules configurations matérielles et logicielles autorisées sont celles mises à disposition par la DSI. Tout équipement qui dérogerait à la règle pourra faire l'objet d'une remise en conformité par la DSI, si elle l'estime nécessaire.

Les matériels mis à disposition fonctionnent avec des logiciels qui ne doivent en aucun cas être désinstallés ni reconfigurés.

Sauf s’il y est autorisé, l’utilisateur ne doit pas modifier les périphériques et les logiciels de communication qui lui sont fournis ou installer de nouveaux équipements non agréés, notamment des points d’accès Wifi (hors Département de la Gironde).

Les équipements n’appartenant pas au Département ne doivent pas être connectés au réseau du Département sur le lieu de travail. Depuis le domicile ou dans le cadre du nomadisme, il existe des connexions autorisées et sécurisées (VPN) avec des accès restreints et la sécurité appropriée.

L’utilisateur d’un ordinateur portable ou d’un appareil mobile Dep33 est tenu de se connecter au réseau du Département au minimum une fois par mois, pour permettre l’exécution des mises à jour des configurations systèmes et antivirus de ses équipements.

À l’intérieur de nos locaux, l’utilisateur d’un ordinateur portable Dep33 doit utiliser la prise du réseau local ou l’accès « Wifi CG33 ». Il ne doit pas se connecter simultanément au réseau du Département et à une carte de connexion sans fil (3G/GPRS, Wifi, ...).

Un ordinateur portable est plus exposé qu’un ordinateur de bureau du fait de sa mobilité.
Son utilisateur doit veiller à ne pas l’exposer au vol en le rangeant sous clé. Il ne doit absolument pas le laisser dans son véhicule. De même, il doit le préserver des chocs, en le transportant systématiquement avec sa housse.

Tout répertoire à caractère privé doit comporter une mention explicite (PERSONNEL) indiquant le caractère privé dans l’intitulé. En l’absence de cette mention, le répertoire sera considéré comme professionnel.

**<u>Le téléphone</u>**

Le Département met à disposition de ses agents des appareils téléphoniques. La ligne standard n'accède qu'aux abonnés girondins et aux portables sur les réseaux de la France métropolitaine.
Les demandes d’évolution de la ligne standard doivent s’effectuer par le catalogue de service DSI.

Les téléphones portables ont un code PIN personnalisé, qui protège l’utilisateur d’une utilisation malveillante (éviter par exemple l’usage des codes PIN du style 0000ou 1234)

Son utilisateur doit veiller à ne pas l’exposer au vol. De même, il doit le préserver des chocs.

Au moment de son attribution, l’utilisateur doit signer une fiche de prêt comportant notamment, le n° d’appel, le code PIN (modifiable), la procédure à suivre en cas de perte ou de vol. L’utilisateur doit prendre toutes les mesures pour que ce document reste entièrement confidentiel.

**<u>Messagerie</u>**

L’utilisateur ne doit en aucun cas s’abonner à des listes de diffusion qui ne relèvent pas de son activité professionnelle.

L’utilisateur ne doit pas donner suite aux demandes de rediffusion de messages de type « chaînes ». Concernant l’envoi de pièces jointes, la taille est automatiquement limitée.

L’utilisateur ne doit pas ouvrir les pièces jointes si l’émetteur est inconnu. La taille du répertoire individuel de la messagerie étant limitée, il appartient à l’utilisateur de supprimer les messages anciens devenus inutiles et d’archiver régulièrement ses messages professionnels.

La messagerie ne doit pas être utilisée pour communiquer des propos diffamatoires, injurieux, xénophobes, sexistes, homophobes ou racistes et d’une manière générale des propos contraires à l'ordre public et aux bonnes mœurs. Tout manquement ou injures par le biais de forums électroniques ou de messagerie est une atteinte flagrante au respect des personnes.

Tout utilisateur qui désire autoriser l'accès à des tiers à sa boite aux lettres ne peut le faire qu'au travers d'une délégation.

Tout dossier ou message à caractère privé doit comporter une mention explicite (PERSONNEL) indiquant le caractère privé dans l'intitulé. En l'absence de cette mention, le dossier ou message sera considéré comme professionnel.

En cas de force majeure, l'accès à la messagerie par une autre personne pour des besoins de services incontournables devra être préalablement validé par le Directeur Général des Services, sur demande du Directeur de la personne concernée. Le processus à suivre pour la consultation de la boîte doit être demandé à la DSI.

**<u>Internet</u>**

Une vigilance particulière est demandée dans l'utilisation de certains services sur internet. Toute requête vers un site web transporte l'identité de la collectivité et donc implique celle-ci.

La navigation sur internet doit se faire en respect de règles de « bonne conduite » :
La connexion aux sites dont les contenus (images, vidéos, écrits) ont un caractère illicite est interdite.

Tout téléchargement illégal ou consultation de sites illicites exposent le contrevenant à des sanctions pénales.

# Protection des données

L'utilisateur protège son environnement de travail, les données et les informations auxquelles il a accès ou qu'il diffuse, par l'emploi adapté de moyens de protection mis à sa disposition (mot de passe sécurisé et non communiqué, verrouillage de session, connexion au réseau pour les itinérants pour mise à jour de l'antivirus…).

Les données professionnelles partageables doivent être stockées sur des répertoires du réseau et dans le cas où l'utilisateur travaille sur son répertoire « D:\Données », il a la responsabilité de la gestion de ses sauvegardes professionnelles. En cas de perte de ces données, la DSI ne pourra pas être tenue responsable

**<u>Diffusion de l'information</u>**

Pour toute information disponible dans les systèmes d'information du Département de la Gironde, l'utilisateur doit s'assurer de la possibilité de diffusion avant toute communication à l'extérieur (règles définies par les services ou autorisations spécifiques).

Tout message électronique comportant dans l'adresse de l'expéditeur l'identification du Département engage, si ce n'est la responsabilité de celui-ci, du moins son image. En conséquence, l'utilisateur doit respecter les règles de validation et le formalisme fixés par l'autorité hiérarchique dont il dépend.

**Respect des droits de propriété**

Le principe de la propriété intellectuelle s'applique à tous les éléments manipulés dans le système d'information : textes, documents, sons, images, films, logiciels etc. Chaque utilisateur s'engage à respecter les droits de la propriété intellectuelle de la collectivité, des partenaires et de tout tiers titulaire de ces droits.

**Loi informatique et libertés**

La création de fichiers, traitements ou documents papier contenant des données personnelles est régie par la loi Informatique et Libertés du 6 janvier 78. Avant toute mise en œuvre d'un fichier ou traitement nominatif, l'utilisateur doit se rapprocher du CIL (Correspondant Informatique et Libertés) présent à la DSI.

# Contrôle de l'utilisation

**Modalités de contrôle**

Les accès internet vers les sites illégaux et non autorisés sont bloqués par le système de filtrage qui fait partie de l'infrastructure de sécurité administrée par la DSI et qui est nécessaire pour assurer la bonne protection de notre Système d'Information. En cas d'attaque virale la DSI se réserve le droit de bloquer l'accès à notre Système d'Information et aux sites internet.

**Interventions à distance sur les postes de travail**

Les administrateurs de la DSI peuvent à distance :

- procéder à des inventaires,
- télécharger des mises à jour logicielles,
- prendre la main à distance sur le poste pour un dépannage, après accord de l'utilisateur concerné.

En cas de dégradation de fichier, la responsabilité du technicien ne peut être mise en cause.

**Procédures de contrôle**

En cas de comportement illicite, d'utilisation frauduleuse, de piratage ou d'utilisation personnelle exagérée des moyens de communication, la DSI est habilitée à demander des explications au responsable de l'anomalie constatée, et de lui rappeler les dispositions de la présente charte.
Si les anomalies perdurent, la DSI est tenue d'alerter la Direction Générale; si cette dernière souhaite donner suite, elle peut demander par ordre écrit à la DSI de limiter les ressources techniques de l'utilisateur.

En cas de suspicion d'infraction pénale, elle peut mettre sous séquestre le matériel et saisir le juge des référés.
Les traces informatiques laissées sur les différents systèmes de la DSI ont également valeur de preuve.

# La mise en œuvre de la charte

**Responsabilité des utilisateurs**

Chaque utilisateur reconnaît que toute violation des dispositions de la présente charte ainsi que, plus généralement, tout dommage créé à l'institution ou à des tiers engagera sa propre responsabilité.

**Mesures d'urgence applicables par la DSI**

La DSI peut en cas d'urgence :

- déconnecter un utilisateur, avec ou sans préavis selon la gravité de la situation,
- isoler ou neutraliser provisoirement toute donnée ou fichier manifestement en contradiction avec la charte ou qui mettrait en péril la sécurité des moyens informatiques,
- imposer des limitations (débit réseau, impression, etc…),
- interrompre certains services,
- stopper brutalement toute activité suspecte qui viole les règles d'utilisation du système d'information.

# Sanctions

Un utilisateur qui aura enfreint les règles édictées dans cette charte pourra voir ses droits d'accès aux ressources informatiques du Département suspendus ou supprimés. Le Département de la Gironde se réserve le droit d'exercer une action en justice à son encontre, dans le respect des textes et règlements en vigueur et en particulier du statut de la fonction publique territoriale..

En application du code de la propriété intellectuelle, l'utilisation et/ou la reproduction sans autorisation de logiciels ou d'œuvres protégées par des droits d'auteur (images, photos, dessins, logos, musique, films, vidéos, etc…) sont constitutifs du délit de contrefaçon susceptible d'entraîner la responsabilité pénale et civile de l'utilisateur.

En fonction de la gravité, l'utilisateur peut être sanctionné tant sur le plan professionnel que sur le plan judiciaire.
Tout manquement à la présente Charte exposerait les utilisateurs à voir leur responsabilité engagée en cas d'infraction pénale ou de faute civile.