ANNEXE 5b

CONSEIL DÉPARTEMENTAL BAS-RHIN

> AGIR AU CŒUR DE VOS VIES

CHARTE TIC

POUR LES COLLABORATEURS DU CONSEIL DÉPARTEMENTAL DU BAS-RHIN

FÉVRIER 2016

sommaire

1.Préambule

Les outils du système d'information sont un vecteur de simplification des démarches administratives, et plus globalement un facteur d'efficience pour les missions quotidiennes des équipes du Conseil Départemental du Bas-Rhin.

Les Technologies de l'Information et de la Communication (TIC) ?

Les TIC regroupent les techniques utilisées dans le traitement et la transmission des informations, principalement de l'informatique, de l'Internet et des télécommunications. Il s'agit des outils permettant de produire, transformer ou échanger de l'information tels les ordinateurs, les téléphones portables, les réseaux et leurs logiciels bureautiques et logiciels métier associés.

Pourquoi une charte ?

La charte a pour but de fixer des **règles générales d'utilisation et d'administration des systèmes d'information de la collectivité**. Cet outil juridique et technique, mais aussi opérationnel, va permettre de guider les utilisateurs dans l'emploi des technologies qui sont mises à leur disposition. Son objectif est de faire respecter les lois et règlements encadrant les activités informatiques et de télécommunications, d'assurer le bon fonctionnement du système d'information, d'en conserver son intégrité et la confidentialité des données détenues par la collectivité, tout en organisant la sécurité juridique des pratiques et des données.

Compte tenu des risques liés à l'utilisation de ces systèmes, il est nécessaire d'informer les utilisateurs afin de mieux garantir la sécurité des ressources informatiques, de télécommunications, des données numériques et technologiques de la collectivité. La charte s'inscrit dans ce cadre pour que soient respectés et adaptés les intérêts en présence, notamment la vie privée des utilisateurs et le respect des obligations incombant nécessairement à l'utilisateur tel que défini dans l'article 2.2 ci-dessous.

Il est rappelé à tous les utilisateurs de ces systèmes d'information que certains usages sont pénalement répréhensibles et que d'autres peuvent nuire au bon fonctionnement du réseau informatique ou sont susceptibles d'engager la responsabilité de la collectivité comme de l'utilisateur.

2. Cadre général

2.1. Définitions

On entend par « **Utilisateur(s)** », les personnes visées à l'article 2.2 de la présente charte.

On désigne par « **Collectivité »,** la personne morale du Département du Bas-Rhin qui met des outils de communication électronique à disposition des Utilisateurs dans le cadre de leurs fonctions respectives.

Toutes les autres définitions sont dans le glossaire en annexe 3 de la présente charte.

2.2. Champ d'application

2.2.1. Les Utilisateurs

Il s'agit de toute personne amenée à utiliser les moyens de communications électroniques mis à disposition par la collectivité :

- **les élus,**
- **les agents titulaires, et non titulaires**
- **les agents liés à la collectivité par un contrat de travail de droit privé,**
- **les stagiaires,**
- **les apprentis.**

2.2.2. Les moyens

Il s'agit de tout système d'information ou de communication. Sont notamment concernés les ordinateurs, logiciels, messageries, accès à Internet/intranet/extranet, téléphones… La charte est valable aussi bien sur les postes fixes que sur les postes nomades ou les connexions à partir de l'outil de travail fourni par la collectivité à l'utilisateur.

Les moyens matériels et logiciels mis à disposition des Utilisateurs demeurent la propriété du Département du Bas-Rhin, et sont mis à disposition de l'Utilisateur dans la seule finalité d'exécuter les tâches et missions qui lui sont confiées par la collectivité.

Chaque Utilisateur est responsable des moyens qui lui sont confiés.

S'agissant de la mise à disposition de ces moyens aux élus, l'article L.3121-18-1 du Code général des collectivités territoriales, dispose que « *le conseil départemental assure la diffusion de l'information auprès de ses membres élus par les moyens matériels qu'il juge les plus appropriés. Afin de permettre l'échange d'informations sur les affaires relevant de ses compétences, le conseil départemental peut, dans les conditions définies par son assemblée délibérante, mettre à disposition de ses membres élus, à titre individuel, les moyens informatiques et de télécommunications nécessaires* ». Il s'agit d'une mise à disposition à titre individuel pour chaque conseiller(e) départemental(e) qui n'est pas cessible.

2.2.3. L'usage

Des risques existent quant à l'intégrité du réseau et du système d'information, l'Utilisateur constitue à ce titre un des piliers garant de sa sécurité. De ce fait, un usage conforme des TIC aux règles établies doit être respecté.

- Utiliser l'intranet, les extranets et l'Internet comme des outils professionnels et non à des fins personnelles, lucratives ou non, dans le cadre de ses attributions et fonctions ;

- Utiliser l'intranet, les extranets et l'Internet comme des outils de communication et des vecteurs d'information ;

- Respecter les spécifications techniques relatives à l'utilisation du logiciel ou progiciel utilisé ainsi que celles relatives à la sécurité en termes de fichiers attachés, compressés ou non, quelle que soit la nature des données (textes, sons, images fixes ou animées…) ;

- Respecter les notices techniques relatives à la mise en œuvre des ressources ;

- Respecter la confidentialité des données échangées.

L'Utilisateur est responsable de l'usage qu'il fait des moyens, des ressources informatiques et du réseau informatique mis à sa disposition par la collectivité dans l'exercice de ses fonctions.

3. Sécurité du système d'information et de communication

Les portails Internet/Intranet et Extranet sont les premiers à être confrontés à des attaques malveillantes. Des outils sont mis en place pour protéger les ressources du système d'information de la Collectivité afin d'en assurer la confidentialité et d'éviter au maximum les conséquences que pourraient engendrer de telles attaques (dysfonctionnement informatique, vol ou modification de données sensibles, saturation de la bande passante…).

3.1. Rôle de l'administrateur système et réseau

L'administrateur du système et du réseau du Conseil Départemental du Bas-Rhin est un agent de la Direction des Systèmes d'Information (DSI), auquel a été confiée explicitement la responsabilité d'un système informatique, d'un réseau informatique ou de télécommunication.

A ce titre, il a pour mission d'assurer le bon fonctionnement et la sécurité du réseau, et est responsable de l'intégrité du système.

Il met en place et gère par conséquent tous les outils nécessaires à cette surveillance et à la protection de toute intrusion, pollution ou acte hostile.

L'administrateur est tenu par une obligation de confidentialité et à un strict respect du secret professionnel.

Sans préjudice de la confidentialité des correspondances, l'administrateur est toutefois 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 TIC.

Parmi les outils utilisés, les logiciels de prise de main à distance peuvent notamment permettre à l'administrateur d'accéder à l'ensemble des données de n'importe quel poste de travail, à des fins de maintenance informatique ou de dépannage.

Ces logiciels ne sont en aucun cas utilisés par la Collectivité aux fins de contrôles de l'utilisation des moyens par les utilisateurs.

Et dans l'hypothèse d'un recours à ces outils à des fins de maintenance informatique par un administrateur, leur utilisation garantit la transparence dans leur emploi et la confidentialité des données auxquelles

il accédera par ce moyen. Cet accès se fait nécessairement dans la stricte limite de ses besoins.

Dans le cas d'une prise en main à distance, l'administrateur prend la précaution d'informer préalablement l'Utilisateur et de recueillir son accord pour lui « donner la main » avant l'intervention sur son poste (l'accord est donné par l'Utilisateur par simple validation d'un message d'information apparaissant sur l'écran de l'Utilisateur).

Dans l'intérêt de la Collectivité et pour les missions dévolues à l'Utilisateur, l'administrateur pourra être amené à effectuer, à distance, des installations de logiciels.

3.2. Conditions d'accès et d'identification

L'ensemble des règles exposées dans cet article a pour but d'assurer la sécurité de tous. L'application de ces mesures permet de se prémunir de tous risques et notamment de toute atteinte grave telle que l'usurpation d'identité.

L'Utilisateur ne doit en aucun cas accéder aux ressources en utilisant l'habilitation d'un tiers. L'Utilisateur ne devra donc pas masquer sa véritable identité en se connectant sous le nom et le mot de passe d'un autre Utilisateur.

A ce titre, chaque Utilisateur se voit attribuer un nom d'Utilisateur personnel, non transmissible, pour un usage exclusif et sécurisé du système d'information du Département du Bas-Rhin.

L'Utilisateur doit **garder confidentiels ses mots de passe, identifiant** (nom d'Utilisateur), clés privées, cartes, etc… et ne pas les dévoiler ou les laisser à la disposition des tiers. Chaque Utilisateur est propriétaire de son mot de passe. Le choix du mot de passe ne doit pas être simple ou facilement déductible et être notamment différent du numéro d'identification, du nom ou prénom de l'Utilisateur, des prénoms de ses enfants ainsi que de sa date de naissance et de son numéro de téléphone interne, personnel ou mobile… Il est exclu de l'inscrire sur tout support (papier ou électronique) à proximité des outils informatiques mis à disposition ou sur ceux-ci, ainsi que de le stocker en clair dans un registre, un programme ou un fichier, afin d'éviter qu'il soit directement accessible.

L'Utilisateur veillera à changer son mot de passe au minimum une fois par an, ou mieux, deux fois par an. Il est libre de le faire à tout moment mais,

en tout état de cause, quinze jours avant la date anniversaire, le système préviendra l'Utilisateur qu'il doit changer son mot de passe.

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

L'Utilisateur doit également veiller à toujours verrouiller ou fermer sa session lorsqu'il n'est pas présent sur son poste de travail.

L'Utilisateur doit aussi veiller à ne pas laisser des supports informatiques en évidence (CD-Rom, clés USB, …) ou tout autre support contenant des informations ou des données confidentielles.

Le branchement de tout appareil ou périphérique (du type disque dur externe, graveur, clé USB, carte réseau Wifi, etc.) sur les prises du poste de travail (portable ou PDA) est autorisé, mais demande à l'Utilisateur une vigilance particulière en termes de sécurité pour ne pas porter atteinte à l'intégrité des systèmes d'information.

L'Utilisateur devra avertir[1], dans les plus brefs délais, la Direction des Systèmes d'Information (DSI) de tous dysfonctionnements logiques et techniques constatés et de toutes anomalies découvertes (exemple : intrusion dans le réseau) afin qu'elle s'attache à isoler le dysfonctionnement. L'Utilisateur devra également avertir son supérieur hiérarchique.

3.3. Relations entre Utilisateurs

L'environnement de travail, et plus particulièrement les documents enregistrés sous « Mes documents » ou dans l'espace personnel privé d'IRIS, n'étant accessible à aucun autre Utilisateur, l'Utilisateur doit veiller à déposer les documents susceptibles d'être consultés ou modifiés par d'autres Utilisateurs dans un espace partagé de l'intranet (IRIS) ou dans un répertoire partagé (sur X:), pour remédier aux aléas afférents aux absences et éviter de pénaliser les autres Utilisateurs dans l'avancement de leur travail.

À défaut, il existe une procédure de demande d'accès en cas d'absence d'agent correspondant à la mise à disposition, pour une durée déterminée, d'un lien pointant vers les dossiers professionnels, ou la messagerie de cet

[1] Pour contacter la DSI, envoyez un mail à assistance.dsi@bas-rhin.fr

agent. Cette procédure doit constituer un cas de force majeure et doit émaner du chef de service ou du directeur exclusivement. La DSI n'est pas responsable de la consultation des dossiers désignés.

L'Utilisateur doit nécessairement respecter les libertés publiques. A ce titre, chaque Utilisateur porte une attention particulière quant à l'émission de messages, textes ou images qui pourraient être provocants, malveillants, menaçants, diffamatoires ou qui pourraient porter atteinte à l'intégrité, à la dignité ou à l'image des personnes. L'Utilisateur doit également respecter ses obligations administratives telles que la probité et le devoir de réserve.

L'Utilisateur s'engage à utiliser dans ses messages un style clair, concis et respectueux vis-à-vis du destinataire.

3.4. Préservation de la confidentialité et respect du secret professionnel

L'Utilisateur a une obligation générale et permanente de confidentialité et de discrétion attachée à l'utilisation des informations et documents électroniques disponibles sur le système d'information de la Collectivité, et ce, pour la sauvegarde du patrimoine et des intérêts de cette dernière.

Plus particulièrement, « les fonctionnaires doivent faire preuve de discrétion professionnelle pour tous les faits, informations ou documents dont ils ont connaissance dans l'exercice, ou à l'occasion, de l'exercice de leurs fonctions. »[2]

Dans l'exercice normal de leurs fonctions, les administrateurs systèmes et réseaux peuvent avoir accès à l'intégralité des données du système d'information (cf. § 3.1). La préoccupation de la sécurité du réseau justifie ainsi que les administrateurs réseaux fassent usage de leurs fonctions et des possibilités techniques dont ils disposent pour mener les investigations et prendre les mesures que cette sécurité impose. Les administrateurs réseaux ne divulguent aucune information couverte par la confidentialité des correspondances privées des Utilisateurs, sauf s'ils sont contraints de le faire du fait d'une disposition législative spécifique.

Cette règle de confidentialité s'applique également aux Utilisateurs disposant de droits d'accès spécifiques sur un ensemble de postes de

[2] Extrait de l'article 26 de la loi du 13 juillet 1983 relative aux droits et obligations des fonctionnaires.

travail, tels par exemple les référents informatiques d'un service ou d'une direction.

Par ailleurs, certaines personnes dépositaires d'informations sont tenues, par la loi, au secret professionnel (exemple : médecin,….). En qualité d'Utilisateur, les dispositions de la présente charte leur sont toujours applicables.

Lorsque l'information ou les données concernées sont couvertes par le secret professionnel au sens de la loi, il appartient aux Utilisateurs qui en sont émetteurs ou destinataires de créer un dossier spécifique intitulé « Secret Professionnel prénom.nom ». Les personnes concernées n'y stockeront que les données, fichiers, dossiers dont le contenu est soumis au secret professionnel. Exemple : si l'Utilisateur s'appelle Bernard Point, il enregistre ses données et fichiers dans un dossier « Dossier Secret Professionnel bernard.point ». Ce cas s'applique par exemple aux médecins exerçant leur fonction au sein de la Collectivité.

Dans le cadre de l'utilisation de la messagerie électronique, l'Utilisateur dont les correspondances sont soumises au secret professionnel, en tant qu'émetteur mais également en qualité de récepteur, s'engage à avertir son correspondant que ledit message est couvert par le secret professionnel. En ce sens, l'Utilisateur s'engage à informer son correspondant de la nécessité pour ce dernier de mentionner dans l'objet de son message les termes « Secret Professionnel : … ». L'Utilisateur devra stocker ses messages dans un dossier spécifique Outlook dénommé « Dossier Secret Professionnel prénom.nom ».

L'Utilisateur reconnaît que si les données et fichiers ne sont pas identifiés comme soumis au secret professionnel (absence d'intitulé spécifique) par celui-ci ou ses émetteurs, ils seront considérés comme des données ou fichiers professionnels accessibles à tous. Si ces données ou fichiers sont identifiés comme « privés », les dispositions décrites au § 4.1 s'appliquent.

3.5. Conditions d'utilisation des systèmes d'information

Tout agissement de l'Utilisateur doit être mesuré. Son comportement est présumé professionnel sans que cela ne nuise pour autant au respect de sa vie privée. Dès lors une part résiduelle d'exercice de ces libertés est admise et garantie, cela dans un équilibre répondant à des attitudes socialement admises telles que : appeler l'école si un enfant est malade, effectuer une déclaration d'assurance suite à un accident… Toutefois la

DSI peut exercer un contrôle des zones privées lorsqu'il existe un risque de remise en cause du bon fonctionnement des systèmes d'information.

3.5.1. Pérennité des ressources

L'Utilisateur ne doit pas apporter de perturbations au fonctionnement des ressources que ce soit par l'adjonction ou la suppression d'équipements matériels ou logiciels ou par la modification des données nécessaires à leur fonctionnement ou par l'introduction d'un logiciel malveillant (virus, cheval de Troie, etc.).

Il est formellement interdit de copier des logiciels d'autres Utilisateurs ou d'utiliser des logiciels dont la collectivité n'a pas acquis les licences d'exploitation.

L'Utilisateur ne doit pas débrancher d'élément nécessaire à l'infrastructure du système d'information tels qu'un câble réseau, borne Wi-Fi, fils électriques de quelque nature que ce soit (liste non exhaustive), sans accord de la DSI. L'Utilisateur ne doit pas modifier l'environnement de son poste de travail ni la configuration de ses ressources car il risque de détruire les éléments nécessaires à la conservation, à la transmission ou au traitement des informations.

L'administrateur du réseau se réserve la possibilité d'interrompre la connexion Internet afin de garantir la sécurité et la stabilité du système.

L'ensemble des données saisies et mises en forme par l'Utilisateur dans le cadre de ses missions appartient à la collectivité. L'Utilisateur ne doit pas détruire les fichiers ou les documents sur lesquels sa fonction et ses missions le conduisent à intervenir avant de s'être assuré que cette destruction ne porte aucun préjudice à la Collectivité ou sans avoir obtenu, préalablement à la destruction, le visa écrit du directeur des Archives départementales. Il respectera les règles d'archivage définies par la Collectivité. Ces règles d'archivage sont issues d'une obligation légale puisque, dans ce contexte, les archives créées par voie électronique sont des archives publiques au sens du Code du patrimoine. Les règles applicables en la matière trouvent ainsi à s'appliquer. Chaque Utilisateur doit veiller à les respecter. Pour plus d'informations, l'Utilisateur est invité à s'adresser aux Archives départementales.

L'Utilisateur doit, en outre, sauvegarder régulièrement les données qu'il exploite, qu'il crée ou qu'il transforme pour assurer la continuité du

service. Il est pleinement responsable de la sauvegarde de ses productions à l'aide des outils mis à disposition à cet effet.

3.5.2. Conditions d'accès et de consultation des TIC mises à disposition

- MESSAGERIE ELECTRONIQUE

Par principe, la messagerie électronique professionnelle est disponible dans la seule finalité d'exécuter les tâches et missions qui sont confiées à l'Utilisateur par son administration. De ce fait, tout message rédigé ou reçu par un Utilisateur sur sa messagerie professionnelle est présumé revêtir un caractère professionnel. L'Utilisateur peut être amené, de manière exceptionnelle et/ou urgente, à utiliser la messagerie à des fins personnelles. L'Utilisateur doit ainsi faire preuve de mesure : il ne doit pas en abuser, ni dans le nombre de courriels personnels envoyés ou reçus, ni par le temps qu'il y consacre, sur son temps de travail. Dès lors il s'engage à marquer les messages privés qu'il envoie par l'intitulé « PRIVÉ », et à classer ceux qu'il reçoit et souhaite conserver dans un dossier spécifique dénommé « Dossier Privé prénom.nom » sous Outlook. Tout message ne comportant pas un tel intitulé, ou non classé dans ce dossier particulier, est présumé professionnel.

Au vu du risque accru de propagation d'un virus informatique par le biais de systèmes de messagerie personnel basé sur le web (tels que Yahoo, Orange, Gmail, Hotmail…), leur utilisation n'est pas autorisée à partir des postes de travail de la collectivité.

La Collectivité met à disposition de l'Utilisateur une messagerie permettant les communications internes entre les Utilisateurs sous le suivi des administrateurs. L'adresse de la boite aux lettres de l'Utilisateur se présente sous la forme suivante: prénom.nom@bas-rhin.fr ou structure@bas-rhin.fr. L'Utilisateur est ainsi identifié, mais il doit cependant insérer à la fin de chaque message sa signature électronique ou son identification professionnelle (telle que nom, prénom, fonction, adresse professionnelle électronique).

L'Utilisateur s'engage à être vigilant vis-à-vis des mails envoyés (notamment quant à la pertinence du choix des destinataires) et à respecter les principes de la discrétion et du secret professionnel mais aussi ceux du respect de ses supérieurs, de ses collègues et de son administration.

L'Utilisateur respectera les règles de fonctionnement internes à son organisation, en utilisant la règle des copies pour informer sa hiérarchie le cas échéant.

L'Utilisateur s'interdit d'envoyer des messages en «masse» («spamming») et de répondre à des «chaines de messages». Il évitera de ce fait de voir sa responsabilité engagée et d'encombrer le réseau ainsi que sa messagerie. Il s'engage également à ne pas ouvrir les messages lui semblant suspects, ou ceux pour lesquels il a des doutes sur l'émetteur et/ou le contenu.

Selon la nature du danger potentiel, l'Utilisateur peut, soit débloquer lui-même le message suspect et, ce faisant, il engage **sa responsabilité** quant au contenu du message, soit demander par mail à la DSI[3], le déblocage du message. Il lui est également permis de créer une liste blanche afin de rendre fiable des expéditeurs précis qui ne seront plus bloqués à l'avenir.

Pour des raisons de sécurité, les messages et les fichiers comportant un virus ou étant chiffrés sont adressés au destinataire après suppression de la partie infectée lorsque cela est possible. Lorsqu'il s'agit de problèmes affectant les messages sortants, l'Utilisateur et la DSI sont immédiatement avisés, ainsi que l'administrateur.

La taille des fichiers joints aux courriers électroniques ne peut dépasser 20 Mo, sauf droit exceptionnel mis en place par la DSI.

Il est fortement recommandé de procéder à la création de dossiers d'archivage. Il est parfois nécessaire de garder une trace de certains échanges, l'assistance de la DSI recommande dès lors à l'Utilisateur vigilant d'effectuer une sauvegarde quotidienne, ou au moins hebdomadaire.

Attention : Les messages stockés dans la catégorie « dossier privé » ne sont pas sauvegardés. Il appartient par conséquent à l'Utilisateur de prendre ses dispositions pour conserver ses dossiers privés.

Enfin, l'Utilisateur veillera à activer le gestionnaire d'absence de sa messagerie électronique en cas d'absence planifiée, et à le désactiver dès

[3] Pour contacter la DSI, envoyez un mail à assistance.dsi@bas-rhin.fr

son retour au bureau. Le message d'absence indiquera la période d'absence, ainsi que la ou les personnes à contacter.

- CALENDRIER ELECTRONIQUE

L'Utilisateur dispose d'un calendrier électronique qu'il doit utiliser pour gérer ses rendez-vous et réunions. Ces agendas doivent être partagés entre les responsables et leurs subordonnés, et peuvent être partagés au sein d'une équipe de travail.

Le caractère public (mode « lecture : disponibilité ») du calendrier partagé permet le bon déroulement des échanges professionnels. Il est conseillé, le cas échéant, de préciser si le rendez-vous est privé de telle sorte que le créneau soit bloqué sans que son contenu soit diffusé pour autant. Ce système permet une meilleure planification des rencontres de travail.

- WEB

Un accès individuel à Internet et à l'intranet est attribué à chaque Utilisateur doté d'un outil informatique. Il comporte des sites libres d'accès et des sites nécessitant une authentification préalable qui ne font pas toujours l'objet de barrières techniques efficaces.

S'inscrire sur un site WEB non reconnu par le Département peut amener l'Utilisateur d'une part à être victime de l'envoi massif de messages, et d'autre part à voir son poste de travail pollué par des raccourcis Internet et autres applications non souhaitées.

Il est donc interdit à l'Utilisateur d'accéder à un site nécessitant notamment une authentification même dans le cas où cet accès apparaîtrait techniquement possible, à l'exception des sites extranets du Département du Bas-Rhin, des applications nécessaires au bon fonctionnement du service public ou des sites pour lesquels le Département a souscrit un abonnement particulier (Ex. : marchés publics en ligne).

Au même titre que la messagerie, il existe ici une présomption de « professionnalité ». Par conséquent, toute connexion établie pendant le temps de travail grâce à l'outil informatique mis à disposition par la Collectivité pour l'exécution du travail est censée avoir un caractère professionnel. **L'utilisation privative n'est pas interdite mais doit être raisonnable** et non susceptible d'amoindrir les conditions d'accès professionnel au réseau. L'Utilisateur doit ainsi faire preuve de mesure dans l'usage d'Internet : il ne doit pas en abuser, ni dans le nombre de

connexion, ni par le temps qu'il y consacre, sur son temps de travail. Des outils légaux de suivi de la navigation sur le web sont mis en place pour des exigences de sécurité, de prévention, ou de contrôle, notamment de l'encombrement du réseau. Ainsi il existe une sélection et un filtrage de sites non autorisés, qui vont être bloqués d'office, notamment tous ceux définis dans le périmètre illégal français (sites à caractère pornographique, pédophile, ou diffusant du contenu incitant à la haine raciale par exemple).

Par exception et sur demande motivée adressée à la DSI[4], et toujours dans un contexte professionnel, l'accès à un site bloqué, non réprimé par la loi pourra être autorisé.

- FORUM ET CHAT

Les forums de discussion permettent la réunion de plusieurs Utilisateurs des réseaux Internet sur un thème précis.

L'Utilisateur est informé des risques liés à l'utilisation de ces modes de communication notamment quant à l'engagement de sa responsabilité dans les propos émis dans le cadre de sa participation à un forum ou un « chat ».

Dès lors, l'Utilisateur n'est pas autorisé à utiliser ces modes de communication en dehors de la stricte nécessité de ses fonctions au sein de la Collectivité, ou en cas de mise en service d'un « chat professionnel » par la collectivité.

Il est strictement interdit à l'Utilisateur de diffuser vers l'extérieur des informations ou données confidentielles ayant trait à l'activité de la Collectivité, et il ne doit en aucun cas faire mention à travers cet outil de toute donnée personnelle le concernant. L'Utilisateur est informé qu'il n'est procédé à aucun enregistrement de message instantané, l'information restant volatile.

- RESEAUX SOCIAUX

Les sites de réseaux sociaux constituent des services en ligne permettant aux individus de se construire un profil public ou semi-public, et d'établir une liste d'Utilisateurs avec qui ils peuvent interagir et communiquer. Il

[4] Pour contacter la DSI, envoyez un mail à assistance.dsi@bas-rhin.fr

s'agit de tout site permettant à un Utilisateur de diffuser un message, ou une quelconque information à un groupe de personnes. Exemple : Facebook, Twitter, LinkedIn, Viadéo…

Au même titre que la messagerie, il existe ici une présomption de « professionnalité ». Par conséquent, l'activité sur les réseaux sociaux aux heures de travail, pendant le temps de travail grâce à l'outil informatique mis à disposition par la Collectivité pour l'exécution du travail, est censée avoir un caractère professionnel. Toutefois, l'**utilisation privative n'est pas interdite mais doit être raisonnable.**

Le comportement des agents sur ces réseaux, à leur domicile, relève de leur vie privée mais des recommandations de bon usage doivent être formulées afin d'éviter tout contentieux. À ce titre, les Utilisateurs des systèmes d'informations de la Collectivité doivent user des réseaux sociaux et autres sites avec vigilance et mesure gardée, et cela même à l'occasion d'un usage personnel.

Tout agent peut s'exprimer librement, mais s'il mentionne sa collectivité ou un de ses représentants, il est soumis, même à titre personnel, à une obligation de réserve, de neutralité et de discrétion professionnelle. L'Utilisateur s'engage à **respecter la Collectivité et son image.**

Tout Utilisateur est responsable de ses agissements sur Internet et notamment des propos laissés dans les zones de commentaires libres. Toutes informations personnelles laissées par eux peuvent être collectées par des tiers, la Collectivité n'en assume aucune responsabilité.

- LISTE DE DIFFUSION

Une liste de diffusion constitue un ensemble de destinataires recevant simultanément un même message électronique. Par exemple, la liste de diffusion nommée « 5 Pôle Fonctionnel » permet d'adresser un message à l'ensemble des agents du Pôle fonctionnel. Les lettres d'information ou « newsletter » utilisent ce système.

L'envoi de messages à l'ensemble des Utilisateurs est interdit, sauf autorisation expresse.

Seuls les Directeurs ou les agents agissant par délégation sont autorisés à diffuser de manière générale un message à l'ensemble des agents du Département. Cette possibilité reste toutefois exceptionnelle.

L'inscription sur des listes de diffusion externes est réservée à un usage strictement professionnel. Cette faculté ne doit pas faire l'objet d'abus afin d'éviter la pollution des messageries électroniques.

En outre, l'Utilisateur doit toujours vérifier lors de son abonnement qu'il existe une procédure de désabonnement. Tout Utilisateur peut choisir de s'abonner à une liste de diffusion ou une bibliothèque de documents de l'intranet du Département avec une fréquence définie. Le gestionnaire d'un site du Département peut abonner un groupe à une alerte ou liste de distribution sans accord préalable des Utilisateurs. Toutefois, dès lors qu'un tiers (personne non identifiée comme Utilisateur, externe à la Collectivité) est abonné à une alerte ou une liste de distribution, le gestionnaire du site devra disposer d'un accord écrit (par mail ou par courrier) des membres du groupe. Un Utilisateur peut à tout moment résilier un abonnement à une alerte ou liste de distribution de l'intranet du Département, et ce, sans justification aucune.

- PLATEFORMES D'ECHANGE DE FICHIERS

Ces outils permettent d'échanger des données avec des partenaires extérieurs (via la création de compte permettant ensuite de créer ou de modifier des éléments à partager). Les fichiers diffusés via ces plateformes doivent être professionnels et demeurent sous l'**entière responsabilité des Utilisateurs**, dans le respect des règles de confidentialité. Toute diffusion de contenu infecté ou bien protégé par des droits de propriété intellectuelle (droits d'auteur par exemple) est prohibée.

- PROTOCOLE DE TRANSFERT DE DONNEES

Un tel protocole permet le téléchargement de fichiers. Mais ceux-ci peuvent comporter des virus préjudiciables au bon fonctionnement du système d'information de la Collectivité.

Le téléchargement de logiciels est également source de risques tant techniques que juridiques. Les règles qui suivent tendent à protéger la Collectivité et les Utilisateurs, notamment contre d'éventuelles actions en contrefaçon.

Ainsi, tout téléchargement de fichiers autres que des documents d'informations depuis le réseau Internet est strictement interdit, sauf autorisation expresse de la DSI. De même, le téléchargement de logiciels est soumis à l'autorisation expresse de la DSI. Elle procèdera à des

vérifications en termes de sécurité informatique et de licence d'utilisation. En cas d'autorisation de téléchargement, l'Utilisateur veillera à respecter strictement les conditions d'utilisation du logiciel dans le cas où ces licences sont consenties à titre gratuit. Les logiciels doivent être utilisés exclusivement dans les conditions des licences souscrites par la Collectivité.

L'utilisation des ressources informatiques et informationnelles de la Collectivité implique le respect des droits de propriété des fournisseurs et des tiers. L'Utilisateur doit respecter les droits de propriété attachés aux informations ou aux données dans le cadre de l'utilisation de l'intranet, des extranets et d'Internet.

L'Utilisateur s'interdit également toute reproduction et utilisation de fichiers, données ou bases de données de tiers protégés par le droit de la propriété intellectuelle ou un droit privatif (cf. Annexe 1).

3.5.3. Conditions d'utilisation du matériel informatique et technologique mis à disposition

Le nombre d'Utilisateurs équipés d'outils « mobiles » (PDA, ordinateur portable, tablette tactile …) croît d'année en année. Pour garantir la sécurité du système d'information, il incombe aujourd'hui aux Utilisateurs équipés de veiller à quelques précautions et règles de sécurités définies ci-dessous.

- ORDINATEURS PORTABLES

Tous les postes (fixes et portables) mis à la disposition des Utilisateurs dans les différents sites du Conseil Départemental du Bas-Rhin sont soumis à la présente charte.

Tout Utilisateur qui bénéficie d'un ordinateur portable confié par la Collectivité dans le cadre de l'exercice de ses fonctions doit, d'une manière générale en prendre soin, et lorsqu'il ne l'utilise pas, le ranger dans un endroit sécurisé et fermé à clé. Il ne doit en aucun cas le céder à un tiers pour que celui-ci l'utilise.

Lors de déplacements, l'Utilisateur doit veiller à ne pas laisser l'ordinateur apparent dans un véhicule.

En cas de vol de l'ordinateur portable confié, l'Utilisateur doit effectuer une déclaration auprès du commissariat de police le plus proche, et ce

dans les plus brefs délais, et appliquer la procédure en vigueur dans la Collectivité, et disponible auprès de l'assistance de la DSI.

Toute déclaration volontairement fausse est passible de sanctions disciplinaires et/ou pénales.

Aucun ordinateur extérieur et non confié par la Collectivité ne doit être connecté au réseau local de la Collectivité (hors réseau Wifi Public).

Lorsque l'Utilisateur est connecté sur le réseau, il ne se connecte à Internet que via le réseau de la Collectivité. A cet égard, il s'engage notamment à ne pas avoir recours à des réseaux WIFI externes qui seraient accessibles durant sa connexion au réseau du Département.

Les postes mobiles disposent d'un client VPN permettant d'établir une connexion automatique au réseau du Département depuis l'extérieur. L'Utilisateur ne doit pas modifier cette configuration, sauf autorisation exceptionnelle de la DSI.

L'Utilisateur doit régulièrement veiller à ce que son logiciel anti-virus soit à jour (fichier de définitions de virus datant de moins d'un mois), et plus particulièrement s'il s'agit d'un ordinateur portable qui n'est pas régulièrement connecté au réseau informatique de la Collectivité.

L'Utilisateur évitera de conserver des documents confidentiels sur tout système de stockage de données externes (disque dur externe, carte SD, clé USB, …)

Le respect de ces obligations protège l'Utilisateur contre les cas de divulgation d'informations confidentielles susceptibles de lui être imputés.

- TELEPHONIE

L'Utilisateur s'engage à n'utiliser les outils de téléphonie mis à sa disposition par la Collectivité que dans le cadre des missions qui lui sont imparties par cette dernière. Il s'engage en outre à limiter ses communications au strict nécessaire, en privilégiant le téléphone fixe (et non le téléphone mobile), en limitant la durée des conversations et le nombre de SMS envoyés.

En dehors du cadre exclusivement professionnel, l'Utilisateur pourra pour des raisons personnelles utiliser ces divers moyens mis à sa disposition par la Collectivité, mais seulement de manière exceptionnelle ou pour une raison commandée par l'urgence. **L'Utilisation privative n'est pas**

interdite mais doit être raisonnable. L'Utilisateur doit ainsi faire preuve de mesure dans son utilisation privée de la téléphonie (fixe ou mobile) pendant les heures de travail.

Les flux téléphoniques sont contrôlés au même titre que ceux du Web à des fins de sécurité et de vérification comptable. Ce contrôle s'opère de façon à garantir le respect de la vie privée et des libertés des Utilisateurs ainsi que selon les préconisations de la CNIL.

La durée de conservation des données relatives à l'utilisation des services de téléphonie est fixée à un an.

- VISIOCONFERENCE

Le système de visioconférence peut être mis en place dans les salles spécialement dédiées à cet effet ou bien dans les bureaux des Utilisateurs. Chacun des participants en entrant dans une salle de visioconférence, est informé de fait qu'il peut bien entendu être filmé. Ainsi il est considéré comme l'ayant accepté et manifeste par là son consentement à être filmé.

Toute session de visioconférence est susceptible d'être enregistrée. Les droits des participants sont garantis, particulièrement les droits d'information, de rectification ou d'opposition pour des motifs légitimes. Chaque enregistrement est susceptible d'être publié sur l'intranet de la Collectivité, ainsi que sur le site institutionnel.

Les séances publiques du Conseil Départemental du Bas-Rhin enregistrées dans le cadre de la visioconférence peuvent être retransmises, comme le précise la loi[5], par des moyens de communication audiovisuelle.

Tout autre usage des enregistrements issus d'une visioconférence peut être prévu et inséré dans une clause contractuelle, notamment concernant la publication sur Internet et l'intranet.

- RESEAU WIFI PUBLIC

Le Conseil Départemental du Bas-Rhin met à la disposition des visiteurs désireux de se connecter à Internet, un réseau Wi-Fi dit « public ». Les Utilisateurs visés par la présente charte ne sont pas concernés par ce réseau, qui est régi par des conditions générales d'utilisation propres.

[5] Article L3121-11 du Code Général des Collectivités territoriales.

4. Suivi des Informations et des moyens de communication

4.1. Suivi et traçabilité des informations

Chaque connexion (totale ou partielle telle une tentative), notamment la navigation sur Internet, les extranets et l'intranet, fait l'objet d'un suivi et d'une traçabilité. Outre le filtrage des sites non autorisés, un suivi individuel (poste par poste et Utilisateur par Utilisateur) est exercé sur les sites et les pages visités, les éléments téléchargés, ainsi que leur nature.

De même, un suivi, une traçabilité et une vérification des messages et fichiers sont effectués, étant rappelé que tout message émis ou reçu depuis le poste mis à disposition de l'Utilisateur par la Collectivité, revêt un caractère professionnel, sauf indication contraire manifeste dans l'objet du message (présomption de « professionnalité ») ou dans le nom du répertoire d'archivage. Il en va de même pour les fichiers de l'Utilisateur. L'identification du caractère privé des mails et des fichiers suppose en effet un acte positif de la part de l'Utilisateur.

A cet égard, l'Utilisateur s'engage à intituler correctement ses dossiers et à classer ses documents ou fichiers personnels dans un dossier nommé « Dossier Privé prénom.nom » dans le dossier « Mes documents ».

La Collectivité s'interdit d'ouvrir ou faire ouvrir les messages ou fichiers identifiés par l'Utilisateur comme « Privés » contenus dans le dossier dédié et dans la messagerie, ou tout autre support mis à disposition de l'Utilisateur par la Collectivité, sauf dans les cas autorisés par la loi et/ou la jurisprudence. Notamment, en cas de risque ou évènement particuliers tel que par exemple une infraction pénale, de non respect avéré ou suspecté de la présente charte ou des lois en vigueur, le Département (DRH – DSI) se réserve le droit de convoquer l'Utilisateur pour l'ouverture du (des) message(s) ou du (des) fichier(s) marqué(s) « Privé(s) » et suivra la procédure ci-après.

L'Utilisateur peut alors être convoqué selon la procédure décrite en annexe 2.

L'accès quotidien par les Utilisateurs à Internet et à l'intranet du Département génère un journal d'exploitation contenant des informations à caractère personnel et horodatées sur la navigation (par exemple : utilisation des éléments et documents publiés sur l'intranet).

Enfin, pour la même finalité, l'utilisation de téléphones fixes, mobiles et PDA mis à disposition par la Collectivité fait également l'objet d'un suivi et d'une traçabilité, notamment en ce qui concerne les numéros appelés, les dates, heures et durées des communications. Des informations peuvent ainsi être transmises aux responsables de service à des fins statistiques et de contrôle du respect de la charte. Le détail des communications pourra être fourni à un Utilisateur sur sa demande.

La durée de conservation de l'ensemble de ces données est précisée à l'article 3.

Les administrateurs peuvent contrôler l'utilisation qui est faite des moyens mis à disposition, afin de vérifier la conformité à leur objet. Conformément aux dispositions prévues par la loi Informatique et Libertés du 6 janvier 1978 modifiée et la déclaration CNIL, les administrateurs peuvent être amenés à réaliser :

- des rapports individuels (statistiques de navigation) transmissibles à l'utilisateur lui-même,
- ou des rapports génériques non personnalisés transmissibles à la hiérarchie.

Les administrateurs réseau ont légalement un devoir d'alerte de la hiérarchie lorsqu'ils constatent qu'un Utilisateur ne se conforme pas aux dispositions de la charte. En cas de non-respect ou de suspicion de non-respect, la collectivité est amenée à demander aux administrateurs réseaux la réalisation d'un rapport personnalisé de nature à vérifier le respect de la charte, conformément aux dispositions prévues par la loi Informatique et Libertés du 6 janvier 1978 modifiée et de la déclaration CNIL. En cas de non-respect constaté des dispositions de la charte et en fonction de la gravité de la violation, une sanction pourra être prise contre l'Utilisateur conformément à l'article 5.2 ci-après.

4.2. Collecte des informations et sauvegarde

L'Utilisateur s'engage à respecter la législation en matière d'informations sensibles dont la collecte et le traitement sont interdits par la loi dès lors que les informations sont relatives à la race ou à l'ethnie, aux opinions politiques, philosophiques ou religieuses, à l'appartenance syndicale, aux mœurs, à la santé et à la vie sexuelle ou encore portent atteintes à l'intégrité, la réputation, la vie privée ou la sensibilité d'un autre Utilisateur, notamment par la mise en ligne de messages, d'images ou de textes à caractère pornographique.

La Collectivité s'engage à ce que les données concernant les Utilisateurs soient collectées et traitées de manière loyale conformément à la loi « Informatique et libertés » du 6 janvier 1978 modifiée.

Les informations concernant les Utilisateurs sont destinées aux personnes habilitées par la Collectivité. L'Utilisateur est informé qu'il dispose d'un droit d'accès et de rectification dans les conditions suivantes :

- l'Utilisateur dispose d'un droit d'accès aux informations nominatives le concernant, ainsi que du droit de rectification le cas échéant, dans les conditions de la loi informatique, fichiers et libertés du 6 janvier 1978 modifiée par la loi du 6 août 2004 ;

- ce droit d'accès et/ou de rectification s'exerce auprès de la Direction des Ressources Humaines.

Il existe une obligation légale de détention et de conservation des données de connexion à laquelle est soumise la collectivité, notamment à des fins préventives en cas d'ouverture d'une instruction judiciaire, ainsi qu'à des fins de sécurité, de vérification et de statistique, la mise en place d'un système de filtrage et de suivi (art. 6-II de la Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique)

Les sauvegardes de ressources sont conservées conformément au Décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne ainsi qu'aux déclarations faites dans le respect des mesures imposées par la CNIL et tel que détaillé à l'article 3.5.

4.3. Vie privée des Utilisateurs

La vie privée des Utilisateurs, mais également celle des agents sous astreinte est respectée et garantie dans le cadre de l'utilisation des moyens de communications et d'information mis à leur disposition par la Collectivité.

Cependant l'Utilisateur doit faire preuve de professionnalisme et faire principalement usage de ces différents moyens dans le cadre des missions qui lui sont confiées par la Collectivité. L'usage personnel des moyens mis à disposition doit s'exercer avec mesure, dans les limites imposées par le bon fonctionnement du service.

4.4. Relations collectives de travail

Les représentants du personnel sont considérés comme des Utilisateurs au sens de la présente charte dès lors qu'ils font usage des moyens mis à leur disposition par la Collectivité.

Toutefois, l'activité de représentant du personnel en tant que telle peut conduire à des spécificités, par exemple en matière de listes de diffusion. Des aménagements spécifiques pourront être passés pour la catégorie d'agents « représentants du personnel ». Le cas échéant, ces aménagements devront être formalisés par écrit.

En ce qui concerne les activités syndicales, l'utilisation des outils informatiques et des moyens de communication électronique dont l'intranet, est soumise au respect des modalités fixées dans un accord passé avec la Collectivité[6]. La mise à disposition des publications et tracts de nature syndicale sur l'intranet de la Collectivité ne peut se faire que dans le cadre de la rubrique qui est dédiée à cet effet. Les organisations syndicales peuvent utiliser la messagerie électronique pour leurs relations de travail avec l'administration ou pour la correspondance avec un agent.

5. Usage responsable des TIC

5.1. Opposabilité de la Charte

La charte est opposable aux Utilisateurs, tels qu'ils sont désignés par l'article 2.2.1, en cas de litige notamment. Elle possède une force contraignante et sa violation – une utilisation non autorisée ou détournée des TIC - peut aboutir à une sanction disciplinaire voire pénale de l'Utilisateur.

À ce titre, la Collectivité invite les Utilisateurs à transmettre à la DSI[7] toutes les difficultés qu'ils pourraient rencontrer.

5.2. Responsabilité des Utilisateurs et sanctions

La responsabilité de l'Utilisateur s'appréciera au cas par cas, dans le respect des textes en vigueur, en fonction de la nature et de la gravité des faits reprochés.

---

[6] Protocole d'accord en vigueur sur l'application du droit syndical au Conseil Départemental du Bas-Rhin

[7] Pour contacter la DSI, envoyez un mail à assistance.dsi@bas-rhin.fr

Il est rappelé à l'Utilisateur que l'engagement de sa responsabilité sera appréhendé selon son appartenance à une catégorie.

En cas de non-respect des dispositions de la charte par un Utilisateur, notamment dans l'utilisation des moyens informatiques mis à disposition, et en fonction de la gravité de la violation, que cette violation résulte d'un manquement unique ou répété, l'Utilisateur pourra faire l'objet :

- d'un rappel à l'ordre verbal,
- d'un rappel à l'ordre écrit par la voie d'un courrier simple,
- d'une restriction d'utilisation ou d'une suppression temporaire de l'utilisation d'un ou plusieurs moyens informatiques,
- d'une sanction disciplinaire issue de l'un des quatre groupes comme le dispose l'article 89 de la loi n° 84-53 du 26 janvier 1984, pouvant aller du simple avertissement à la révocation.

En outre, selon l'article 29 de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires, « toute faute commise par un fonctionnaire dans l'exercice ou à l'occasion de l'exercice de ses fonctions l'expose à une sanction disciplinaire sans préjudice, le cas échéant, des peines prévues par la loi pénale ».Il est précisé que toute sanction disciplinaire à l'encontre d'un agent public Utilisateur sera :

- prise sur la base d'un faisceau d'indices probants ;
- nécessairement proportionnée à la gravité de la faute commise.

6. Lois applicables

L'ensemble de la législation applicable figure en annexe 1 de la présente charte

7. Modalités d'application de la charte

7.1. Entrée en vigueur

Après délibération de la Commission Permanente en date du 7 janvier 2013 et l'arrêté du Président du Conseil Départemental en date du 18 janvier 2013, le Conseil Départemental du Bas-Rhin met en application la présente charte d'utilisation des TIC à compter du 2 avril 2013.

7.2. Mise à jour et évolution

Ce document remplace et abroge les précédents documents émis par la collectivité relatifs à l'utilisation des ressources informatiques, informationnelles, numériques et technologiques dont il est question dans la présente charte.

La DSI proposera une mise à jour dès que des modifications s'avèrent nécessaires.

La mise en place d'une nouvelle version s'effectue uniquement après consultation du comité technique paritaire et délibération de la Commission Permanente.

7.3. Transmission et accès

La présente charte est portée à la connaissance de chaque Utilisateur par tous moyens adéquats et notamment par : la diffusion sur l'intranet (tout nouvel Utilisateur devra accepter de prendre connaissance de la présente charte à la 1ère connexion), l'ajout d'une annexe au règlement intérieur, aux conventions de stages.

Chaque Utilisateur destinataire de la présente charte est invité à transmettre à la DSI[8] toutes propositions de modifications ou d'ajouts dont il a pu constater l'intérêt dans le cadre de sa pratique des systèmes d'information.

[8] Pour contacter la DSI, envoyez un mail à assistance.dsi@bas-rhin.fr

Annexe 1 – REGLEMENTATION APPLICABLE

Cadre Général

- Les règles générales de la transparence, de la concertation et du respect mutuel ;
- La protection des personnes inscrites dans les bases de données du Conseil Départemental du Bas-Rhin ;
- La protection de l'intégrité technique des systèmes d'information du Conseil Départemental du Bas-Rhin.

Particularités administratives

- La loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires ;
- La loi n° 84-53 du 26 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale
- Le Code Général des Collectivités Territoriales
- La loi n° 94-665 du 4 août 1994 relative à l'emploi de la langue française

Respect de la vie privée et des droits d'autrui

- L'article 9 du Code Civil et l'article 8 de la Convention Européenne de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales ;
- La loi n° 91-646 du 10 juillet 1991 garantissant la protection par la loi du secret des correspondances émises par la voie des télécommunications ;
- Les articles 226-1,226-15 (pour le secteur privé) et 432-9 (pour le secteur public) du Code Pénal incriminant le fait de porter atteinte à l'intimité de la vie privée d'autrui par le moyen d'un procédé quelconque et/ou au secret des correspondances (un an d'emprisonnement et 45000 euros d'amende) ;

- Les lois n° 90-615 du 13 juillet 1990 et n° 92-1336 du 16 décembre 1992 interdisant de faire l'apologie du racisme, de l'antisémitisme et de la xénophobie ;

- La loi du 29 juillet 1881 sur la Liberté de la presse, notamment concernant la diffamation et l'injure.

- La loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique- La loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, dite loi HADOPI. Cette loi a notamment créé une obligation de surveillance par l'article L.336-3 du Code de la propriété intellectuelle (CPI) selon lequel « La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise ». En outre, en qualité de fournisseur d'accès au réseau Internet, le Département a une obligation de sécurisation de cet accès (art. L.335-7, R.335-5 CPI)

- La loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet

- La loi n° 2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure dite LOPSI 1

- La loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, dite loi LOPPSI 2

Règlementations des données à caractère personnel

- Les articles 226-16 à 226-22 du nouveau code pénal sur « les atteintes aux droits des personnes résultant des fichiers ou des traitements informatique» ;

- Les articles 410-1, 411-6 et 432-9 al.1 du Nouveau Code Pénal rappelant 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 ;

- La loi « Informatique et libertés » n° 78-17 du 6 janvier 1978 modifiée.

Responsabilité en cas d'atteinte à un système de traitement automatisé de données

- Loi n° 88-19 du 5 janvier 1988 relative à la répression des atteintes aux systèmes de traitements automatisés de données, dite loi « Godfrain »

- Les articles 323-1 à 323-5 du code pénal s'appliquent en cas d'atteinte à un système de traitement automatisé de données (STAD), ainsi qu'en cas d'accès frauduleux à un système ou lors de l'introduction d'un virus.

Droits de propriété intellectuelle

L'article L.112-1 du Code de la propriété intellectuelle pose le principe de la protection des œuvres de l'esprit dont font partie les œuvres multimédias.

La propriété intellectuelle protège les droits des auteurs ou ses ayants droit sur toutes les œuvres de l'esprit, quels qu'en soient le genre, la forme d'expression, le mérite ou la destination. Cette création doit avoir un caractère « original ».

La propriété intellectuelle sur une œuvre comprend des droits moraux, attachés à la personne de l'auteur de l'œuvre qui sont perpétuels, inaliénables et imprescriptibles, ainsi que des droits patrimoniaux.

Les droits moraux de l'auteur comportent :
- le droit de divulgation c'est-à-dire le droit de divulguer ou non l'œuvre, dans les conditions choisies par l'auteur,
- le droit de paternité c'est-à-dire le droit au nom (ou le droit à l'anonymat ou au pseudonyme),
- le droit au respect de l'œuvre c'est-à-dire le droit de faire respecter l'intégrité de l'œuvre,
- le droit de retrait ou de repentir c'est-à-dire le droit de revenir sur la divulgation (le retrait) ou de modifier l'œuvre (repentir) après divulgation.

Les droits patrimoniaux de l'auteur et de ses ayants droit leur permettent d'être rémunérés pour chaque utilisation de l'œuvre pendant une durée de 70 ans après la mort de l'auteur. À l'issue de cette période de protection,

l'œuvre entre dans le domaine public, et peut être librement utilisée par tous.

Néanmoins, même après l'entrée d'un œuvre dans le domaine public, l'Utilisateur devra tout de même veiller au respect des droits moraux de l'auteur.

Les articles du Code de la propriété intellectuelle concernant le droit d'auteur et les droits voisins, mais aussi les marques, les dessins et modèles, les brevets et les bases de données et tout autre signe distinctif, s'appliquent ainsi pleinement. Toute forme de contrefaçon (reproduction, téléchargement, copie, diffusion, modification…) est prohibée et les Utilisateurs doivent toujours vérifier en amont la disponibilité et la légalité des droits avant une quelconque utilisation.

S'agissant du droit d'auteur, l'absence de consentement exprès des auteurs, ou de leur ayant droit ou ayant cause, caractérise le délit de contrefaçon, prévu par les articles L.335-2 et suivant du Code de la propriété intellectuelle.

S'agissant des marques, l'atteinte portée au droit du propriétaire d'une marque constitue une contrefaçon engageant la responsabilité civile de son auteur tel que prévu par l'article L.716-1 du Code de la propriété intellectuelle.

L'Utilisateur ne doit donc pas reproduire, télécharger, copier, diffuser, modifier ou utiliser les logiciels, bases de données, page Web, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif sans avoir obtenu au préalable l'autorisation des titulaires de ces droits.

L'usage du droit de publication devra ainsi respecter toute réglementation applicable dans ce domaine.

Les droits de propriété intellectuelle afférents à un message en tant qu'œuvre appartiennent à l'émetteur qui en est donc responsable.

L'Utilisateur s'engage par conséquent à ne pas faire une utilisation de fichiers électroniques contraire au droit de la propriété intellectuelle et à ne pas télécharger illégalement des fichiers électroniques sur des sites Internet (vidéo, musique, ...etc).

Annexe 2 – Procédure de convocation d'un Utilisateur dans le cadre de l'article 4.1

L'Utilisateur peut être convoqué par un courrier recommandé avec accusé de réception dans la perspective de l'ouverture du (des) message(s) ou du (des) fichier(s) marqué(s) « Privé(s) ».

Trois situations peuvent alors être envisagées :

- L'Utilisateur décide de venir à la convocation, le cas échéant assisté d'un représentant syndical ou d'une personne du choix de l'Utilisateur : il est alors soumis à la signature de cet Utilisateur un document dans lequel il reconnaît et accepte que ses fichiers personnels soient ouverts en sa présence. Selon les données identifiées, une procédure de sanction disciplinaire peut être engagée à l'encontre de l'Utilisateur. La sanction sera proportionnée à la gravité de la faute ;

- L'Utilisateur ne vient pas ou refuse la convocation : en cas d'infraction pénale soupçonnée, le Département saisira un officier de police judiciaire afin d'ouvrir les fichiers personnels concernés. Toutes les conséquences de droit en seront alors tirées ;

- L'Utilisateur ne vient pas ou refuse la convocation : dans les autres cas avéré (hors infraction pénale soupçonnée) de non respect de la charte, le Département ne procèdera pas à l'ouverture des messages ou fichiers identifiés par l'Utilisateur comme « Privés ». Toutefois, le Département pourra engager une procédure de sanction disciplinaire au regard des indices et autres éléments d'informations dont il dispose. La sanction sera proportionnée à la gravité de la faute.

Annexe 3 - Glossaire

- **Base de données** : Ensemble structuré de fichiers reliés entre eux dans lesquels les données sont organisées selon certains critères en vue de permettre leur exploitation.
- « **chat** » : Communication informelle entre plusieurs personnes sur Internet, par affichage de messages sur leurs écrans de manière instantanée et quasi-simultanée.
- **Client VPN** : Outil permettant de se connecter au réseau informatique de la collectivité depuis l'extérieur (par exemple à domicile ou en déplacement), par l'intermédiaire de réseaux publics (tel qu'Internet), en préservant sa sécurité.
- **CNIL** : Commission nationale de l'informatique et des libertés qui est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Tout système de traitement automatisé de données à caractère personnel doit lui être déclaré.
- **Communications électroniques :** les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique » (Article L. 32 du Code des Postes et des Communications Electroniques).

  Exemples d'outils ou moyens de communication électronique : les téléphones fixes et portables, PDA communicants, Internet, extranets, intranet, messageries, visioconférence …
- **Extranet** : Extension du système d'information de la collectivité permettant de mettre à la disposition de partenaires extérieurs un ensemble d'applications et de services dématérialisés.
- **Internet** : réseau informatique mondial constitué d'un ensemble de réseaux nationaux, régionaux et privés. Il propose principalement les trois services suivants : le courrier électronique, le web (pages avec liens et contenus), et l'échange de fichiers.

- **Intranet** : Réseau local et privé (entreprise ou tout autre entité organisationnelle) qui utilise les technologies de communications d'Internet : Web, e-mail, etc., mais ne s'ouvre pas aux connexions publiques contrairement à Internet. Il sert à communiquer, mais également à formaliser une connaissance à partager (groupware, ou travail collaboratif), à déployer des applications (diminution des coûts et meilleure convivialité pour les Utilisateurs), à suivre des procédures ou processus (Workflow).

- **Logiciel** : Ensemble de programmes, qui permet à un ordinateur ou à un système d'informations d'assurer une tâche ou une fonction en particulier (exemple : logiciel de traitement de texte, tableur, logiciel spécialisé métier…).

- **Outils informatiques** : Matériels et logiciels informatiques mis à la disposition des Utilisateurs par le Département (poste de travail, outils bureautiques, …).

- **PDA :** Un assistant numérique personnel est un appareil numérique portable, qui dispose de surcroît habituellement de fonctions de télécommunication

- **Progiciel** : Logiciel commercial vendu par un éditeur sous forme d'un produit complet, plus ou moins clés en main. Le terme résulte de la contraction des mots produit et logiciel (mot-valise).

- **Spam** : Communication électronique non sollicitée. Il s'agit souvent d'envoi en masse de messages à des fins publicitaires.

- **Statistiques de navigation** : Compte-rendu sur les activités Internet des Utilisateurs

- **STAD** : Système de Traitement Automatisé de Données. Cela concerne l'ensemble des éléments physiques et des programmes employés pour le traitement de données, ainsi que des réseaux assurant la communication entre les différents éléments du système d'information. Il en est ainsi des ordinateurs, mais également des périphériques d'entrée/sortie et des terminaux d'accès à distance, ainsi que de tous vecteurs de transmission de données, tels que les réseaux de communications électroniques.

- **Téléchargement** : Opération de transmission d'informations (programmes, données, images, sons, vidéos) d'un ordinateur à un autre via un canal de transmission, en général Internet.

- **Téléphonie** : Système de télécommunication qui a pour but la transmission de son et en particulier la transmission de la parole. Sont notamment concernés les téléphones fixes et portables, les PDA (assistant numérique personnel) communicants, les télécopies…
- **Visioconférence** : La visioconférence est un outil par lequel des personnes peuvent communiquer entre elles, en temps réel, en utilisant des réseaux de télécommunications, et ceci malgré la distance les séparant.
- **Webmail** : Système de messagerie fonctionnant depuis Internet et faisant office de lecteur mail. Ce système permet l'émission, la consultation et la manipulation de courriers électroniques. Exemples : Gmail, Yahoo!, Windows live Hotmail, Free…
- **Wifi** : Technologie permettant de se connecter sans fil à un réseau local.

INFO+

CONSEIL DÉPARTEMENTAL
BAS-RHIN

CONSEIL DÉPARTEMENTAL DU BAS-RHIN
HÔTEL DU DÉPARTEMENT
Place du Quartier Blanc / 67964 STRASBOURG cedex 9
Tél : **03 88 76 67 67** / Fax : **03 88 76 67 97**

www.bas-rhin.fr

Direction des Systèmes d'Information
Service Assistance et Support
Tèl : 03 88 76 60 00
Mèl : assistance.dsi@bas-rhin.fr
iris : Mon 67 > Outils informatiques > Charte TIC

conception et impression CD67 / février 2016