GRAND DAX AGGLOMÉRATION

GRAND DAX ACTION SOCIALE

CHARTE DE BON USAGE DES MOYENS INFORMATIQUES ET DE TELECOMMUNICATION

PREAMBULE

Le développement des technologies de l'information et de la communication a conduit le personnel et les élus de la communauté d'agglomération et du centre intercommunal d'action sociale du Grand Dax à utiliser dans leur travail quotidien l'outil informatique, les réseaux et les services de communication numériques pour l'exécution de leurs missions.

Cette utilisation peut comporter un certain nombre de risques, d'ordre aussi bien technique que juridique, pouvant engager la responsabilité de la collectivité et de ses agents.

La présente charte, qui se veut avant tout un document d'information et de référence, a ainsi pour objet :

- de déterminer les conditions d'utilisation des moyens ou/et des ressources informatiques mis à disposition,
- de définir les droits et obligations des personnes utilisatrices de ces outils, dans le respect des droits et libertés de chacun,
- d'informer et sensibiliser sur les risques encourus pour les prévenir, et garantir ainsi la sécurité, l'intégrité et la confidentialité des données.

Cette charte est susceptible d'être modifiée régulièrement en fonction des évolutions technologiques et réglementaires, le cas échéant.

Chaque utilisateur s'engage à la respecter.

Sommaire

1.CHAMP D'APPLICATION DE LA CHARTE 3
1.1Les utilisateurs concernés 3
1.2Les systèmes d'information et de communication 3
2.UTILISATION DES MATERIELS ET DES LOGICIELS MIS A DISPOSITION 3
2.1Postes informatiques 3
2.2Poste de travail nomade et tablette tactiles 4
2.3Copieurs numériques multifonctions 4
2.4Poste téléphoniques fixes 5
2.5Téléphones mobiles 5
2.6Logiciels 5
2.7Badges électroniques et pointeuse 6
2.8Signature électronique et certificat 6
2.9Messagerie électronique 6
3.MOYENS DESTINES A ASSURER LA SECURITE INFORMATIQUE 8
3.1Compte « utilisateur » et mot de passe 8
3.2Dispositifs de préventions des virus informatiques 8
3.3Prévention des risques liés à la messagerie électronique 8
3.4Utilisation d'Internet 9
3.5Pare-feu réseau et filtrage des contenus 9
3.6Administration des systèmes d'information et contrôle technique 10
4.DROITS ET DEVOIRS DES UTILISATEURS 11
4.1Principes généraux 11
4.2Respect de la confidentialité des données 12
4.3Utilisation des médias sociaux 13
4.4En cas de départ d'un utilisateur 15
5.MANQUEMENT A LA CHARTE 15
6.OPPOSABILITE DE LA CHARTE 15

1. CHAMP D'APPLICATION DE LA CHARTE

1.1 Les utilisateurs concernés

La présente charte s'applique à toute personne qui, ayant un lien de droit statutaire ou contractuel avec la collectivité, est amenée à utiliser les outils informatiques et moyens de télécommunications mis à disposition par cette dernière, pour satisfaire à ses missions. A noter que les personnes accueillies en stage ou les saisonniers utilisant ces mêmes moyens devront également se présenter à la direction intercommunale des Systèmes d'information (DISI) pour signer cette charte.

Elle est :

- disponible sur l'intranet pour tous les utilisateurs et chaque utilisateur devra signer et remettre à la DISI le récépissé qu'il aura reçu,
- opposable aux tiers utilisant un équipement informatique mis à disposition par la collectivité, à titre permanent ou occasionnel,
- accessible et mise à jour directement sur l'intranet.

1.2 Les systèmes d'information et de communication

Les systèmes d'information et de communication englobent les équipements informatiques, électroniques et téléphoniques de la collectivité, interconnectés ou non entre eux. Il s'agit notamment :

- des ordinateurs (fixes ou portables),
- des périphériques y compris clés USB, assistants personnels, réseaux informatiques (serveurs, routeurs et connectiques),
- des photocopieurs, télécopieurs, imprimantes et scanners,
- des téléphones, smartphones, tablettes et clés 4G,
- des logiciels, fichiers, données et bases de données,
- des systèmes de messagerie,
- des connexions internet, intranet, extranet, abonnements à des services interactifs, etc.

2. UTILISATION DES MATERIELS ET DES LOGICIELS MIS A DISPOSITION

2.1 Postes informatiques

Du matériel informatique est mis à la disposition de chaque utilisateur. Celui-ci est fragile, il convient que chacun en prenne soin. Il comprend (liste non exhaustive) :

- Unité centrale, écran, souris, clavier, ordinateur portable, …
- Système d'exploitation : Windows, Mac OS, …
- Logiciel(s) : pack bureautique, logiciels de communication (messagerie), logiciels métiers spécifiques.

Tout utilisateur s'engage à ne pas effectuer d'opérations qui pourraient avoir pour conséquences :

- de modifier le fonctionnement, le paramétrage et les caractéristiques de son poste de travail informatique (installation de nouveaux matériels, de logiciels même gratuits, modification des fichiers systèmes...) ;
- d'interrompre, même temporairement, le fonctionnement de tout système connecté au réseau (le débranchement ou le déplacement de tout matériel informatique ou téléphonique doit être réalisé par un agent de la DISI ou, à défaut, par une personne expressément habilitée) ;
- d'accéder ou d'essayer d'accéder à des informations privées d'autres utilisateurs du réseau (en utilisant son mot de passe, par exemple) ;
- de modifier ou de détruire des informations communes (partagées par plusieurs utilisateurs) stockées sur le réseau.

L'enregistrement des travaux des utilisateurs doit être réalisé dans les espaces prévus à cet effet : répertoires du service ou d'échange sur le réseau, répertoires personnels sur son poste. Tout document situé hors de ces répertoires pourra être supprimé par les administrateurs du réseau sauf dispositifs spécifiques et/ou contraintes particulières. A noter que les données stockées en local sur les PC ne font l'objet d'aucune sauvegarde.

2.2 Poste de travail nomade et tablette tactiles

Ces équipements peuvent être mis à disposition pour un usage strictement professionnel et ne doivent en aucun cas être utilisés par des personnes ne faisant pas partie de la collectivité et/ou n'ayant pas signé la présente charte. Lorsque ces matériels sont utilisés à l'extérieur, notamment dans le cadre de réunions ou d'intervention hors des locaux de la collectivité, les utilisateurs en assurent la garde et la responsabilité.

Les utilisateurs ont dans cette hypothèse un niveau de surveillance et de confidentialité renforcé et doivent veiller à ce que des tiers non autorisés ne puissent accéder à ses moyens ni les utiliser.

En termes de sécurité et de confidentialité, les utilisateurs sont soumis aux mêmes obligations que les utilisateurs restant sur site. Ils devront suivre toutes les prescriptions complémentaires qui leur seront signifiées.

À l'extérieur de l'enceinte de la collectivité, la connexion à des points d'accès Wi-Fi publics qui ne sont pas de confiance (par exemple à l'hôtel, la gare ou l'aéroport…) est proscrite. Les utilisateurs devront se connecter par le biais des clés 3G/4G ou téléphone (via la fonction de partage de connexion) professionnel mis à disposition.

En cas de dysfonctionnement, de blocage, de perte ou de vol de l'équipement, les utilisateurs doivent en informer immédiatement la direction intercommunale des Systèmes d'information. Ils doivent par ailleurs assister la collectivité, dans toutes les démarches (déclaration d'assurance, dépôt de plainte, etc.) rendues nécessaires à la suite d'un incident de quelque nature que ce soit.

2.3 Copieurs numériques multifonctions

Du fait de leurs fonctionnalités étendues, les copieurs numériques constituent un périphérique dont la sécurité doit être assurée comme celle des postes de travail informatiques. Dès lors que des informations à protéger transitent par ce type d'appareil, l'ensemble des recommandations et réglementations relatives aux systèmes d'informations s'appliquent.

Lors de la numérisation de documents, les utilisateurs doivent s'assurer que la destination des fichiers ainsi générés est accessible aux seules personnes habilitées à accéder à ces informations. Les répertoires de « scan par service » ou la fonction de « scan vers email personnel » sont notamment disponibles pour cette utilisation.

Les utilisateurs doivent s'abstenir de reproduire, copier, diffuser des pages web, images, photographies, textes ou toutes autres créations protégées par le droit d'auteur.

Une sensibilisation est faite aux utilisateurs afin :

- d'éviter l'impression systématique de mails (et notamment en couleur) ou de documents en version provisoire,
- d'utiliser la fonction « aperçu » avant d'imprimer,
- d'utiliser le mode d'impression couleur, uniquement pour les documents contenant des visuels le nécessitant.

2.4 Poste téléphoniques fixes

L'utilisation du téléphone fixe est réservée à des fins professionnelles.
En cas d'absence, les utilisateurs doivent effectuer un renvoi sur le poste d'un autre utilisateur habilité à recevoir et traiter ses appels ou bien sur le service d'accueil du site sur lequel il est basé.

L'usage du téléphone fixe pour des communications personnelles est toléré aux conditions qu'il soit ponctuel, qu'il concerne des appels locaux et n'entrave pas l'activité professionnelle des utilisateurs.

2.5 Téléphones mobiles

Un téléphone mobile peut être mis à la disposition des utilisateurs pour un usage strictement professionnel.

À ce titre, l'utilisateur est tenu :

- d'en prendre soin et de se conformer aux prescriptions d'usage, décrites dans la notice d'utilisation fournie avec le téléphone,
- d'informer immédiatement la direction intercommunale des Systèmes d'information en cas de dysfonctionnement, de blocage, de perte ou de vol de l'équipement.

Il est rappelé que selon le code de la route, l'usage d'un téléphone par le conducteur d'un véhicule en circulation est interdit.

Si le téléphone mobile autorise une connexion à l'internet et à la messagerie, les utilisateurs devront respecter les obligations et interdictions visées au présent points « Internet » et « messagerie » ci-dessous.

A noter que toute utilisation abusive et non professionnelles pourrait faire l'objet de sanction.

2.6 Logiciels

L'utilisateur ne peut installer un logiciel (qu'il soit payant ou gratuit), que ce soit par copie de cédérom, téléchargement ou autre, qu'après accord exprès de la DISI et sous réserve d'une validation préalable d'opportunité formalisée par le responsable auquel l'agent est hiérarchiquement rattaché.

Aucune copie de logiciels n'appartenant pas au domaine public (respect du droit de propriété) n'est autorisée en dehors des copies de sauvegarde. Pour information, l'utilisation et la diffusion de logiciels piratés constituent un délit. Sa diffusion correspond à du recel.

2.7 Badges électroniques et pointeuse

Des utilisateurs disposent de badges électroniques nominatifs et non-cessibles permettant d'accéder aux locaux de la collectivité. Ceux-ci sont connectés aux logiciels de contrôle d'accès des bâtiments concernés qui enregistrent les horaires d'entrées et de sorties.

De la même manière, une pointeuse pour le suivi des horaires de travail des agents est mise en place.

Ces dispositifs ont été portés à la connaissance des utilisateurs avant leur mise en œuvre.

2.8 Signature électronique et certificat

Certains utilisateurs, dans le cadre de leurs fonctions, sont amenés à utiliser des certificats de signature électronique pour signer des documents et/ou s'authentifier pour accéder à des services sécurisés.

Ces certificats sont nominatifs et non-cessibles, ils sont constitués de 3 éléments indissociables :
- les informations concernant l'identité du titulaire, son organisation, sa fonction, la période de validité du certificat et l'identité de l'autorité de certification qui l'a généré,
- la clé privée,
- la clé publique.

L'utilisateur doit ainsi veiller à garder confidentiel le code saisie (clé privée) lors de la signature avec son certificat.

Les certificats ont une durée de validité limitée (3 ans). Toute nouvelle demande de certificat ou de renouvellement doit être validé par le responsable hiérarchique de l'agent et transmis à la DISI.

Les certificats seront révoqués lorsque leur utilisateur quitte la collectivité ou ne dispose plus de l'habilitation à l'utiliser.

2.9 Messagerie électronique

Les utilisateurs disposent d'une boîte aux lettres nominative permettant de recevoir et d'émettre des messages électroniques uniquement professionnels.

Les règles générales d'utilisation :

- L'auteur doit s'identifier en faisant figurer en bas du message son nom, sa fonction et son service, éventuellement son numéro de téléphone. Le modèle de signature mis à disposition et intégré automatiquement aux messages doit ainsi être utilisé par défaut.
- La transmission d'information par la messagerie doit respecter les procédures internes de contrôle, de validation, d'autorisation. Il est souhaitable de mettre systématiquement en copie de message important son responsable et le responsable du destinataire.
- Il est recommandé de vérifier la liste des destinataires avant l'envoi de tout message et d'utiliser la fonction copie cachée (Cci) afin de ne pas rendre le contenu de ces listes accessibles à tous.
- En cas d'absence, doit être activé un message automatique d'absence indiquant la date de retour prévue et éventuellement la personne ou le service à joindre en cas d'urgence.
- Les fichiers joints ne doivent pas dépasser 2 Mo sauf pour des transferts exceptionnels.

- Pour les transmissions de fichiers en interne, il est recommandé de communiquer le chemin d'accès au fichier sur le réseau ou l'intranet dans son message, plutôt que d'envoyer le fichier en pièce jointe.
- Il est recommandé de supprimer rapidement les courriels volumineux sans valeur professionnelle et juridique pertinente, le volume des boites et des courriels échangés étant limité. Les courriels importants devront être stockés et sauvegardés dans le logiciel courrier prévu à cet effet.

La collectivité se réserve le droit d'effectuer des contrôles dans des cas graves de mauvaise utilisation (la liste suivante n'étant pas exhaustive):

- envoyer ou recevoir délibérément des informations et données dont le contenu et la forme peuvent nuire à la collectivité
- envoyer des informations confidentielles sur l'organisation, le personnel et les élus de la collectivité
- envoyer des messages pouvant engager la responsabilité contractuelle de la collectivité

Les mêmes dispositions s'appliquent également pour l'utilisation de boîtes aux lettres professionnelles génériques.

Engagement vis-à-vis des tiers

Un message électronique peut être une preuve ou un début de preuve. Ainsi, en matière commerciale, une preuve peut être apportée par tous les moyens possibles et il y a contrat dès lors que les parties ont donné leur accord sur la chose et sur le prix.
Il est donc rappelé que toutes les recommandations concernant les échanges écrits avec des tiers s'appliquent à la messagerie. Il est donc obligatoire de transmettre pour validation à un responsable tout message qui aurait valeur contractuelle ou qui serait l'expression d'une décision administrative.

Comportement/Actes illicites

Les messages à caractère discriminatoire, faisant état du sexe, de l'état de santé, du handicap, de l'appartenance ethnique ou de l'orientation sexuelle des correspondants sont proscrits. Il en est de même pour les messages faisant apparaître des opinions politiques, philosophiques ou religieuses.

Certes, un agent ne peut être tenu pour responsable s'il reçoit, à son insu, de tels messages mais il lui est imposé de ne pas les relayer. II ne doit donc pas en solliciter l'envoi en participant à des groupes de discussion, ou en consultant des sites, dont le caractère est proscrit, qui pourrait enregistrer ses coordonnées.

Utilisation de la messagerie électronique à des fins personnelles

Il est considéré que tout message reçu ou envoyé à partir du poste de travail mis à la disposition de l'utilisateur revêt par principe un caractère professionnel. L'utilisation de la messagerie à des fins personnelles, lorsqu'elle est rendue nécessaire par les impératifs de la vie courante et familiale, est tolérée si elle n'affecte pas le trafic normal de la messagerie professionnelle.

Le message qui comportera la mention expresse ou manifeste de son caractère personnel bénéficiera du droit au respect de la vie privée et du secret des correspondances. Cependant, l'utilisateur doit être informé de ce que toute activité numérique, comme l'utilisation de la messagerie électronique, laisse des traces et est nécessairement mémorisée. L'utilisateur doit être informé que, pour des raisons de sécurité, d'organisation ou de gestion de l'encombrement du réseau, la DISI peut utiliser des dispositifs d'analyse de messages ou des dispositifs visant à limiter la taille ou le volume des messages échangés. La mise en place de ces dispositifs n'ayant pas pour objet le

contrôle individuel des utilisateurs, la confidentialité des messages sera respectée.

3. MOYENS DESTINES A ASSURER LA SECURITE INFORMATIQUE

3.1 Compte « utilisateur » et mot de passe

Chaque utilisateur du réseau informatique se voit attribuer un *compte* auquel sont associés un identifiant (login) et un *mot de passe*. **Il est responsable de l'utilisation qui est faite de ce compte et il lui appartient donc de ne pas communiquer son mot de passe à une tierce personne. À cet effet, il ne devra être noté sur aucun support et est, de par sa nature, incessible et intransmissible.**

L'utilisateur doit s'identifier clairement. Nul n'a le droit d'usurper l'identité d'autrui ou d'agir de façon anonyme.

L'utilisateur doit quitter son poste de travail en fermant ou en verrouillant sa session (via la combinaison de touches Ctrl + Alt + Suppr ou touche Windows + L). S'il ne se déconnecte pas, sa messagerie et ses répertoires personnels restent accessibles pour tout utilisateur ultérieur sur le poste.

Pour garantir au mieux la confidentialité des fichiers et la sécurité du réseau, la DISI met en place un politique de mot de passe. Elle tient compte des préconisations de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et impose un changement régulier (tous les 90 jours), une longueur et une complexité minimale des mots de passe créés par les utilisateurs.

Le mot de passe doit ainsi comporter au moins 8 caractères dont au moins une lettre en majuscule et une en minuscule, un numéro ou un caractère spécial parmi les suivants : @ % ! | = ( ) ; . : , - + _
Il ne doit pas par ailleurs reprendre le nom ou prénom de l'utilisateur.

3.2 Dispositifs de préventions des virus informatiques

La DISI a mis en œuvre un système antivirus contrôlant les flux externes (Internet) et internes sur le réseau, qui intercepte et élimine les virus informatiques.

Néanmoins, afin de limiter les risques de diffusion de ces virus, il est strictement interdit :
- d'introduire des disquettes, clés USB, CD-ROM ou DVD-ROM venant de sources externes, sans l'accord préalable de la direction intercommunale des Systèmes d'information ;
- de connecter à son postes informatique des équipements personnels : smartphones, tablettes, lecteurs MP3, etc. ;
- d'installer des logiciels externes sans l'accord préalable de la DISI.

Il convient aussi de se méfier des fichiers transmis par messagerie, qui ont un caractère suspect ou provenant d'expéditeurs inconnus (cf. risques liés à la messagerie électronique ci-après). En cas de doute, vous devez vous adresser à la DISI.

En cas de fonctionnement inhabituel de son poste informatique (lenteur du système et/ou du réseau, ouvertures de fenêtres non sollicitées, etc.) il convient de prévenir la DISI.

3.3 Prévention des risques liés à la messagerie électronique

La messagerie est l'un des premiers vecteurs de propagation des virus et de « phishing » (technique utilisée par des escrocs pour collecter des données personnelles). Il est en effet

très simple de diffuser par email un fichier attaché contenant un virus, ou un lien Internet pour inciter à télécharger un programme infecté.

Des outils ont été mis en place pour se prémunir contre ce type d'attaque : tout message infecté détecté par le système de protection sera éradiqué par réparation ou suppression automatique selon les possibilités. Toutefois, il est impossible de garantir un niveau de sécurité total. II est donc nécessaire de respecter la précaution simple suivantes :

- Ne pas ouvrir les messages suspects (non sollicités, ayant un objet douteux, provenant d'un émetteur inconnu ou comportant des liens ou des pièces jointes bizarres), mais les signaler à la DISI pour analyse ou les supprimer directement.
- Ne pas répondre à une demande d'informations confidentielles (mots de passe, code PIN, coordonnées bancaires, etc.) reçue par mail, ceci directement ou en complétant un formulaire en ligne. Jamais la DISI ou « l'administrateur de systèmes informatiques » ne vous demandera ce type d'information par email.
- En cas de doute sur l'expéditeur d'un message, contactez son interlocuteur pour vérifier qu'il est à l'origine du message et ainsi éviter les phénomènes d'usurpation d'identité.
- Prévenir immédiatement la DISI, dans le cas de réception de messages non sollicités récurrents ou manifestement illicites.

3.4 Utilisation d'Internet

Les utilisateurs qui disposent d'un accès à l'Internet pour l'exercice de leur activité professionnelle doivent respecter les prescriptions suivantes :

- ne pas accéder à des sites illicites : sites à caractère pornographique, pédophile, raciste, de jeux d'argent, etc.,
- ne pas accéder à tout site qui pourrait nuire à l'intérêt de la collectivité dans d'autres domaines,
- ne pas télécharger des logiciels, des vidéos, des photos n'ayant aucun lien avec les fonctions et activités professionnelle.

À des fins de sécurité et de vérification du bon accès et usage des ressources du système d'information, la collectivité dispose d'un service de filtrage de contenu Internet (cf. article suivant).

Il est accordé une tolérance à l'accès à des sites Internet à des fins personnelles. Elle est permise dès lors qu'elle reste raisonnable c'est-à-dire limitée dans sa fréquence, sa durée et qu'elle ne nuit pas au bon fonctionnement des services.

3.5 Pare-feu réseau et filtrage des contenus

Les postes raccordés au réseau de la collectivité utilisent un pare-feu dont le rôle est de contrôler les communications entrantes et sortantes depuis ou vers le réseau Internet.

Face aux risques et menaces de plus en plus sophistiquées, un dispositif de filtrage des contenus des sites web visités et de journalisation les communications est ainsi opérationnel dans le but de :

- renforcer la sécurité des systèmes d'information (analyse des menaces, blocage des virus, prévention des intrusions depuis Internet, etc.),
- interdire l'accès à des sites illicites (sites à caractère pédophile, raciste, etc.) ou qui pourrait nuire à l'intérêt de la collectivité dans d'autres domaines,
- assurer une meilleure qualité de service en contrôlant l'utilisation de la bande passante : il est ainsi proscrit de télécharger des logiciels, des vidéos, des photos n'ayant aucun lien avec les fonctions et activités professionnelles,

- empêcher la divulgation d'informations : en effet, dans le cadre de leurs fonctions, les utilisateurs sont amenés à gérer des fichiers dont il est nécessaire de garantir la confidentialité (fichiers contenant des données personnelles notamment),
- protéger : le filtrage n'a pas pour effet de contrôler l'activité sauf dans le cas de présomptions d'infractions aux règles de sécurité énoncées dans la présente charte ou d'abus,
- protéger la collectivité : en effet, dans l'hypothèse où il n'est pas mis en place de solution de filtrage, la responsabilité de la collectivité peut être engagée pour des infractions commises par les utilisateurs dans l'exercice de leurs fonctions (risque civil et pénal),
- respecter les obligations juridiques : différents textes de lois ou références juridiques imposent le recours au filtrage comme la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique qui impose à certains acteurs de mettre en œuvre des moyens de contrôle ou de restriction des accès à internet.

Il est donc formellement interdit aux utilisateurs de modifier, désactiver ou contourner ce dispositif de protection mise en œuvre.

Blocages de sites Internet

Les politiques de filtrages sont été établies sur la base d'un classement par catégories de sites Internet autorisés, bloqués ou soumis à un quota d'utilisation. En cas de blocage, un message d'avertissement apparaît dans le navigateur Internet de l'utilisateur.

Les blocages considéré comme anormaux (faux positifs : sites bloqués mais devant être débloqués pour l'exercice des missions) devront être signalés à la DISI, notamment via l'adresse assistance.informatique@grand-dax.fr

Journalisation des accès

La solution de filtrage permet l'établissement de statistiques par d'utilisateurs, et la génération de journaux selon différents critères :

- temps de navigation,
- bande passante consommée,
- nombre d'accès,
- catégories d'URL consultées.

En cas d'abus ou de doutes sur l'utilisation d'internet, les fichiers sont conservés afin d'engager une procédure interne de contrôle.

Procédure interne de contrôle

En cas de doute ou de présomptions d'infractions ou de connexions abusives pendant les heures de travail, l'autorité territoriale peut interdire ou suspendre l'accès aux ressources prévues et être amené à effectuer des contrôles conformément aux règles édictées dans la présente charte. Tout contrôle et toute sanction font l'objet d'une information préalable de la personne suspectée.

3.6 Administration des systèmes d'information et contrôle technique

La DISI doit assurer le bon fonctionnement des réseaux et des moyens informatiques. Elle peut ainsi effectuer des contrôles techniques sans information préalables de l'utilisateur :

- soit dans un souci de sécurité du réseau et/ou des ressources informatiques : pour des nécessités de maintenance et de gestion techniques, l'utilisation des services, et notamment des ressources matérielles et logicielles, ainsi que les échanges via le

réseau et la messagerie peuvent être analysés et contrôlés dans le respect de la législation applicable, et notamment dans le respect des règles relatives à la protection de la vie privée et au respect des communications privées ;

- soit dans un souci de vérification que l'utilisation des moyens informatiques, de la messagerie et de télécommunication reste conforme aux règles édictées par la présente charte.

En particulier, les administrateurs du réseau disposent d'outils permettant d'analyser tout ce qui transite par celui-ci, notamment :

- les connexions au réseau (identifiants, dates et heures de connexion...) ;
- les fichiers stockés sur les serveurs (format, date, taille...) ;
- les connexions Internet (identifiants de connexion, sites visités, volumes de données transférées, dates et heures de connexion...) ;
- les consommations téléphoniques.

Ces administrateurs sont assujettis au devoir de réserve et sont tenus de respecter la confidentialité des informations auxquelles ils pourraient avoir accès dans le strict cadre de leur mission. Dans ce cadre, l'utilisateur reconnaît accepter expressément les mesures de contrôle mises en œuvre ci-avant exposées.

Cas exceptionnels

Pour assurer la continuité du service public, l'administrateur informatique, sur demande de l'autorité territoriale (DGS uniquement) peut accéder :

- à la messagerie d'un utilisateur absent en respectant la législation en vigueur et sous certaines conditions : il est notamment interdit à quiconque de prendre connaissance d'un message professionnel ayant pour objet « Personnel » ou « Confidentiel », sans l'autorisation expresse de l'utilisateur (qu'il en soit l'auteur ou le destinataire).

- aux fichiers pendant l'absence des utilisateurs ; toute mesure devant être prise pour empêcher l'accès aux données identifiées comme personnelles sur les outils de travail.

Par ailleurs, pour des raisons exceptionnelles de sauvegarde de la sécurité, tous les messages professionnels pourront être ouverts par l'administrateur informatique sur demande écrite de l'autorité territoriale.

4. DROITS ET DEVOIRS DES UTILISATEURS

4.1 Principes généraux

Les utilisateurs doivent :

- appliquer les recommandations de sécurité inscrites dans la présente charte,
- respecter les règles de bon usage afin d'éviter des opérations qui pourraient avoir pour conséquence de nuire à la collectivité,

À ce titre, ils :

- disposent d'un droit d'accès strictement personnel et incessible,
- contribuent à la sécurité informatique, en signalant tout dysfonctionnement ou toute anomalie des ressources qu'ils utilisent,

- utilisent les logiciels dans le respect des règles relatives à la propriété intellectuelle et des droits d'auteur. Ils ne doivent pas reproduire et/ou ne pas diffuser des données soumises à un droit de copie qu'ils ne détiennent pas,
- ne doivent pas introduire de « ressources extérieures » matérielles ou logicielles qui pourraient porter atteinte à la sécurité du système d'information et de communication,
- effectuent des sauvegardes à échéances régulières pour les fichiers autres que ceux déjà sauvegardés automatiquement sur le réseau.

L'utilisation des moyens informatique et télécom doit se limiter à un usage professionnel dans le cadre des missions de service public de la collectivité. Elle doit être réalisée de manière loyale et responsable par tous les utilisateurs.

L'usage à titre personnel doit rester exceptionnel et particulièrement modéré dans sa fréquence et sa durée et ne pas nuire au bon fonctionnement du service.

4.2 Respect de la confidentialité des données

Répartition des droits d'accès aux fichiers

Les utilisateurs sont amenés à gérer, du fait de leurs compétences et dans le cadre de leurs missions, des fichiers dont il est nécessaire de garantir la confidentialité : fichiers d'usagers des services, dossiers individuels et bulletins de paie des utilisateurs, etc.

Ils doivent ainsi veiller :

- à respecter l'intégrité et la confidentialité des données, tant pour la collecte, le traitement et la communication interne et externe des données,
- à ne pas copier ni sauvegarder les fichiers professionnels sur support amovible autres que ceux fournis par la collectivité,
- ne pas collecter des données qui, en raison de leur contenu, contreviendraient aux lois et règlements en vigueur.

Une gestion des droits d'accès est mise en place pour interdire l'accès aux fichiers confidentiels à toute personne autre que le ou les gestionnaires desdits fichiers.

Les utilisateurs s'engagent par ailleurs à ne pas prendre connaissance d'informations appartenant à autrui sans son accord, à ne pas communiquer à un tiers de telles informations ou des informations non publiques auxquelles il peut accéder, mais dont il n'est pas propriétaire.

L'utilisateur est averti que les données enregistrées sur les serveurs de fichiers (lecteurs réseaux M, N, T, etc.) sont partagées avec d'autres utilisateurs, notamment les agents de son service. L'enregistrement de données à caractère personnel et confidentiel sur les serveurs de fichiers mis à disposition est donc proscrit.

Les règles de secret professionnel, de déontologie, d'obligation de réserve et de devoir de discrétion s'imposent concernant les informations présentes sur le réseau et les messages électroniques professionnels.

La protection des données personnelles informatiques

Un nouveau règlement de l'Union européenne, appelé le règlement général sur la protection des données ou « RGPD », accorde aux personnes physiques certains droits relatifs à leurs données personnelles qui sont :

- droit d'accès : le droit d'être informé et de demander l'accès aux données personnelles que la collectivité traite,

- droit de rectification : le droit de demander de modifier ou de mettre à jour les données personnelles lorsqu'elles sont inexactes ou incomplètes,
- droit d'effacement : le droit de demander de supprimer définitivement les données personnelles,
- droit de restriction : le droit de demander d'arrêter temporairement ou définitivement le traitement de tout ou partie des données personnelles,
- droit d'opposition : droit de refuser à tout moment le traitement des données personnelles pour des raisons personnelles, ou pour des fins de marketing direct,
- droit à la portabilité des données : le droit de demander une copie de vos données personnelles au format électronique et le droit de transmettre ces données personnelles pour une utilisation par un service tiers,

La collectivité a pris en compte ces nouvelles directives.

Les utilisateurs peuvent exercer ces droits :

- auprès de Madame la Présidente responsable du traitement de la collectivité,
- ou par écrit en s'adressant au relais du Délégué à la Protection des Données personnelles : relais-dpo@grand-dax.fr.

Le Délégué à la Protection des Données personnelles de la collectivité est l'Agence Landaise Pour l'Informatique (ALPI), 175, place de la Caserne Bosquet BP30069 - 40002 MONT-DE-MARSAN CEDEX), que vous pouvez contacter pour tout renseignement supplémentaire via l'adresse suivante : dpo@alpi40.fr

4.3 Utilisation des médias sociaux

Les outils concernés

Les médias sociaux regroupent tous les sites internet, applications ou plateformes qui permettent aux utilisateurs de créer du contenu, de l'organiser, de le modifier ou de le commenter. Outre les réseaux sociaux, ils peuvent prendre des formes extrêmement variées allant de la messagerie électronique à la diffusion d'actualités en passant par le partage de contenu (texte, photo, vidéo, musique), le commerce en ligne ou les plate-formes de jeux (selon la définition du « web 2.0 »).

Tous les espaces virtuels où l'utilisateur peut être amené à faire un commentaire, interagir ou laisser son empreinte numérique sont concernés.

Utilisés à bon escient, ces outils de communication ouvrent des possibilités nouvelles de contact direct entre l'usager et l'institution. Néanmoins, la facilité d'accès, l'illusion d'anonymat et le sentiment d'impunité qui en découle, la mauvaise connaissance des paramètres de confidentialité, peuvent mettre à mal l'obligation de réserve à laquelle chaque agent est tenu, et l'exposer à des sanctions.

Les médias sociaux doivent ainsi être utilisés avec discernement et engage chacun à respecter des règles de communication.

Le cadre réglementaire général

Le cadre réglementaire général se place dans le champ des infractions définies par le code pénal. Il est ainsi interdit de :
- promouvoir des activités illégales sous quelque forme que ce soit, notamment la copie ou la distribution non autorisée de logiciels, de photos et d'images, le harcèlement, la fraude, les trafics prohibés.
- tenir des propos à caractère diffamatoire, raciste, homophobe, incitant à la violence, à la haine ou à la xénophobie.

- promouvoir la pornographie, la pédophilie, le révisionnisme et le négationnisme.
- publier des contenus contrevenant aux droits d'autrui, incitant aux crimes, aux délits et la provocation au suicide.
- publier des contenus injurieux, obscènes ou offensants
- détourner l'usage d'une page internet pour y exercer de la propagande ou du prosélytisme politique, religieux ou sectaire, ainsi qu'à des fins commerciales.
- dénigrer une collectivité ou un EPCI, des élus, ou des agents.

Les obligations des agents

Les fonctionnaires et agents contractuels sont soumis au devoir de réserve. Cette obligation concerne le mode d'expression des opinions et non leur contenu. Ils sont également soumis à la discrétion et au secret professionnels.

L'obligation de réserve

Tout agent public doit faire preuve de réserve et de mesure dans l'expression écrite et orale de ses opinions personnelles. Cette obligation impose aussi aux agents publics d'éviter en toutes circonstances les comportements susceptibles de porter atteinte à la considération du service public par les usagers. Cette obligation ne concerne pas le contenu des opinions (la liberté d'opinion est reconnue aux agents publics), mais leur mode d'expression. L'obligation de réserve s'applique pendant et hors du temps de service.

Le secret professionnel

Un agent public ne doit pas divulguer les informations personnelles dont il a connaissance. Cette obligation s'applique aux informations relatives à la santé, au comportement, à la situation familiale d'une personne, etc.

La discrétion professionnelle

Un agent public ne doit pas divulguer les informations relatives au fonctionnement de son administration. L'obligation de discrétion concerne tous les documents non communicables aux usagers.

Les précautions à prendre lors de l'utilisation des réseaux sociaux

Les plate-formes sociales sont de véritables espaces publics, visibles et consultables par tous. Tout le monde peut propager vos idées en republiant un contenu écrit, vidéo ou audio instantanément.

Vos conversations, personnelles ou professionnelles, peuvent être diffusées partout sans votre accord. Vous êtes donc impliqué personnellement sur tout ce que vous publiez ou retransmettez (partage, « like », « retweet », commentaire, etc.).

Les informations que vous postez sont indexées par les moteurs de recherche. Elles laissent des traces durables qui peuvent vous suivre tout au long de votre vie, si vous n'agissez pas à temps.

Prenez ainsi quelques minutes de réflexion avant de publier un contenu.

Même si ces réseaux sont des lieux de liberté d'expression, restez prudents : exprimez-vous en toute connaissance des sujets traités.

Soyez respectueux des autres et de leur vie privée. Ne diffusez pas d'information ou ne citez pas de personnes sans leur accord. Ne photographiez pas des personnes sans leur autorisation. Lorsque vous publiez une image ou une photo, n'oubliez pas de mentionner

son auteur et assurez-vous d'avoir préalablement obtenu l'accord des personnes photographiées.

Les propos injurieux, racistes, xénophobes, homophobes… n'ont pas leur place sur Internet, ni dans les réseaux sociaux.

4.4 En cas de départ d'un utilisateur

Tout utilisateur, lors de la cessation de son activité au sein de la collectivité, perd son habilitation à utiliser les systèmes d'information internes.

Il doit :
- restituer tous les matériels mis à sa disposition,
- effacer de son poste de travail tous ses éventuels fichiers et données privés.

Il ne peut effectuer une copie de son travail professionnel qu'après autorisation écrite de son supérieur hiérarchique dûment habilité.

Les éventuels répertoires personnels ainsi que les données de messagerie des utilisateurs situés sur le serveur seront obligatoirement supprimés par l'administrateur informatique, en tout état de cause dans un délai maximum d'un mois après son départ.

5. MANQUEMENT A LA CHARTE

Le non-respect des règles édictées dans cette charte peut amener la collectivité à suspendre, voire supprimer, l'accès des contrevenants à ces outils de communication.

En fonction de la gravité, des sanctions disciplinaires peuvent être prises selon la réglementation en vigueur dans la fonction publique territoriale et une procédure pénale peut être engagée.

6. OPPOSABILITE DE LA CHARTE

La présente charte est rendue opposable dès sa notification à chaque utilisateur valant acceptation entière de ses termes

La Présidente

Mme Elisabeth Bonjean

Charte éditée le 3 octobre 2019,
Présentée au comité technique du 16 octobre 2019.

PRINCIPAUX TEXTES DE REFERENCE

Le règlement (UE) 2016/679, relatif à la protection des personnes physiques à l'égard du traitement des données à caractères personnel et à la libre circulation de ces données,

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et libertés,

La loi n°78-17 du 06/01/78 dite « Informatique et liberté » modifiée par la loi n°2018-493,

La loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques,

La loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique,

La législation relative à la propriété intellectuelle,

La législation relative à la fraude informatique,

La législation en matière de transmission d'informations à caractère violent, pornographique ou de nature à porter gravement atteinte à la dignité humaine et à la diffusion de contenus illicites à caractère injurieux, diffamatoire, raciste, xénophobe, révisionniste et sexiste (articles 227-23 et 227-24 du code pénal et loi du 29 juillet 1881),

Le décret n°2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques,

La loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique,

Les dispositions du code pénal relatives à la fraude informatique et aux atteintes aux droits de la personne et notamment les articles 226-1, 226-15 à 226-24, 321-1 à 323-7,

L'ensemble des dispositions statutaires et notamment la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires et la loi n° 84-53 du 26 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale,

Les dispositions du code du travail relatives à l'information préalable des salariés sur l'existence des moyens et dispositifs de contrôles mis en place, notamment les articles L. 121-8 et L. 432-2-1,

La circulaire du 12 mars 1993 relative aux modalités de l'application de la loi "informatique et libertés" au secteur public,

Le guide d'hygiène informatique - Agence nationale de la sécurité des systèmes d'information – Janvier 2017

_____

RECEPISSE DE LA CHARTE INFORMATIQUE

Je soussigné(e)

Nom – Prénom : .....

Direction/Service : .....

en tant qu'utilisateur du système d'information et de communication de la communauté d'agglomération du Grand Dax et du CIAS du Grand Dax, déclare :

- avoir pris connaissance de la charte disponible sur l'intranet de la collectivité *GDInfos* (adresse internet : http://intranet.grand-dax.fr)*
- m'engage à la respecter pendant toute la durée de mes fonctions, et sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.
- m'engage à prendre connaissance des modifications de cette dernière directement sur l'intranet *GDInfos*.

Fait à ..... Le ……

Signature du bénéficiaire, précédée de la mention « Lu et approuvé »

Ce récépissé est à retourner à la direction intercommunale des systèmes d'information suite à sa signature.

* Utilisez les identifiants personnels qui vous ont été communiqués pour vous connecter à l'Intranet *GDInfos* (identifiants identiques à ceux de votre messagerie professionnelle) puis saisissez « charte informatique » dans le moteur de recherche. Dans le cas où vous n'arriveriez pas à visualiser cette charte sur l'intranet, merci de bien vouloir contacter le service d'assistance à l'adresse assistance.informatique@grand-dax.fr