Charte des usages numériques et du système d'information de Val de Garonne Agglomération

Table des matières

Préambule

Le développement des réseaux, l'utilisation croissante des technologies de l'information et la mise en place d'un cadre juridique plus adapté induisent, progressivement, une nouvelle forme d'organisation et de gestion des relations au sein des administrations, et à l'égard des usagers grâce, par exemple :

- à la mise en ligne d'informations pour plus de transparence ;
- à la mise en place d'intranets pour une meilleure communication entre les utilisateurs et les services,
- à la mise en place d'extranets (intranet de l'Agglo.) dans le cadre de partage d'informations avec des partenaires/usagers.

L'utilisation de tout système d'information suppose de la part des utilisateurs et des administrateurs le respect d'un certain nombre de règles afin d'assurer la sécurité et les performances des traitements, la préservation des données confidentielles dans le respect de la règlementation européenne de la protection des données

C'est pour ces raisons que la Communauté d'Agglomération Val de Garonne a défini une charte numérique qui spécifie les règles que doivent respecter les agents et les élus.

La méconnaissance de la législation, l'ignorance des risques encourus ou une mauvaise application de règles parfois simples et de bon sens, mais toujours essentielles, peuvent être lourdes de conséquences pour la collectivité comme pour chaque agent, dans la mesure où sa responsabilité individuelle pourrait être également engagée.

Il s'agit bien d'une démarche d'organisation qui implique nécessairement toute la collectivité:

- de l'utilisateur qui utilise et qui se trouve de ce fait au centre de la démarche,
- de la Direction Générale et l'encadrement qui assurent le management de la Collectivité et décident du bien-fondé de la demande d'un agent et également de la bonne utilisation au quotidien des moyens mis à sa disposition,
- des services qui participent à la gouvernance de la charte, DSI, service juridique, service numérique, service communication et RH.
- du Délégué à la Protection des Données (DPO) et du comité technique en charge du respect de la protection des données personnelles (COTECH RGPD*).
- Les services (DGS, service juridique, service RH, service communication, service numérique et DSI participants à la gouvernance de la charte auront en charge le suivi et l'évolution de la présente charte (Comité de pilotage de la Charte).

Cette charte est un guide qui s'impose à tous les utilisateurs, validé par le Conseil communautaire, et annexé au règlement intérieur de la collectivité.

Son application au quotidien est l'affaire de tous, dans l'intérêt de chacun.

**COTECH RGPD (Comité technique du Règlement Général de la Protection des Données) qui comprend VGA (DGS, Service des usages numériques, DSI, Service juridique, service communication), Mairie de Marmande, Mairie de Tonneins, CFP (Cité de la Formation Professionnelle), CCAS de Marmande, CCAS de Tonneins et l'Office de Tourisme du Val de Garonne.*

1- Objet et champs d'application

Cette charte s'applique à l'ensemble des moyens de communication et des ressources

informatiques et numériques, quelles que soient les formes sous lesquelles ils sont exploités (carte d'accès, électronique, imprimée, manuscrite, vocale, image…).
Elle a pour objet :

- de faire prendre conscience de la problématique sécuritaire et de responsabiliser chaque utilisateur, individuellement,
- de mettre en évidence la nécessité, pour la sécurité de tous, de respecter cette charte
- de clarifier les droits, les devoirs et les responsabilités des utilisateurs (élus, agents communautaires, prestataires…),
- d'adopter les comportements de sécurité qui sont nécessaires.

Les principes énoncés ne sont pas exclusifs de l'application des lois, du règlement intérieur de la collectivité, des devoirs incombant aux agents, et des règles minimales de courtoisie et de respect d'autrui.

Ensemble des ressources

- Application métiers, bureautiques, messagerie, internet, intranet, extranet
- Données, adresse électronique, comptes réseaux et sociaux
- PC fixes, PC portables, Tablettes, périphériques notamment imprimantes, clés USB, périphériques, scanners…
- Téléphones fixes, mobiles, Fax, photocopieurs.
- Carte d'accès

Liste non limitative qui évoluera en fonction des usages

Ensemble des utilisateurs

- Agents contractuels (de droit privé, de droit public,….) et les personnes intervenant dans le cadre des vacations, stagiaires, agents stagiaires et titulaires, et le Cabinet mutualisé.
- Elus

Liste non limitative qui évoluera en fonction des usages

Les prestataires, partenaires et tout utilisateur du système d'information externe à la collectivité se verront proposer une charte spécifique qui sera annexée au contrat ou à la convention qui les lient à la collectivité.

Patrimoine informationnel

Qu'il s'agisse d'informations administratives, techniques, financières, il constitue l'un des actifs les plus importants de VGA sur lequel repose sa capacité à développer de véritables compétences dans le domaine relevant de ses missions de service public.
Il recouvre :

- Les services d'information nécessaires au plein exercice de ses métiers ;
- Les informations relatives aux usagers ou aux tiers avec lesquels VGA est en relation dont l'altération ou la divulgation pourrait porter atteinte à son image de marque, celle des usagers ou des tiers concernés.
- Les informations qu'il incombe à VGA de conserver en raison d'une obligation règlementaire, de l'intérêt historique ou technique qu'elles peuvent présenter.
- Les informations relatives à ses agents dont la divulgation constituerait une violation de la vie privée.

2. Legislation

Chaque agent est personnellement responsable de son utilisation des moyens

informatiques. A ce titre, il peut voir sa responsabilité individuelle engagée du fait d'une mauvaise utilisation.

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

- Le Code Pénal, notamment ses articles 323-1 à 323-7 relatifs à la fraude informatique.

- Le Code de la propriété intellectuelle qui reconnaît les logiciels comme œuvre de l'esprit et, à ce titre, les protège sans nécessité de dépôt ou d'enregistrement.

- Loi n°83-634 du 13 juillet 1983 modifiée portant droits et obligations des fonctionnaires et la loi n°84-53 du 26 janvier 1984 modifiée portant dispositions statutaires relatives à la fonction publique territoriale, imposant notamment les obligations de réserve, de discrétion et de secret professionnel des agents publics.

- Loi n°78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés, qui a notamment pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'emploi de l'informatique et d'encadrer l'utilisation des données à caractère personnel dans les traitements informatiques.

- Loi n°94-665 du 4 août 1994 modifiée, relative à l'emploi de la langue française.

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril, dit Règlement Général sur la Protection des Données (RGPD) qui constitue le texte de référence en matière de protection des données à caractère personnel.

- Décret n°85-397 du 3 avril 1985 modifié relatif à l'exercice du droit syndical dans la fonction publique territoriale

Télétravail

- Article 133 de la loi n° 2012-347 du 12 mars 2012 modifiée a consacré la possibilité pour les agents publics (fonctionnaires ou non) d'exercer leurs fonctions dans le cadre du télétravail.
- Décret n°2016-151 du 11 février 2016 relatif aux conditions et modalités de mise en œuvre du télétravail dans la fonction publique.

Réseaux sociaux

- Déclaration des droits de l'homme et du citoyen de 1789
- Code pénal : Article R621-1
- Loi du 29 juillet 1881 modifiée relative à la liberté de la presse (art. 32 et 33)

Selon la loi, l'utilisateur DOIT *[liste non exhaustive]* 	Selon la loi, l'utilisateur NE DOIT PAS *[liste non exhaustive]* 
• **Respecter les règles applicables à**	- **Chercher à porter atteinte**

la fonction publique territoriale : >secret professionnel >obligation de réserve >devoir de discrétion, …. Par exemple, respecter les règles relatives à la protection des données nominatives, notamment les informations relatives à la matrice cadastrale. • Répertorier les fichiers de données à caractère personnel	**directement ou indirectement aux droits des personnes physiques** (comme morales) ainsi qu'à leur vie privée, (protection des libertés individuelles et des personnes, respect du secret des correspondances) - **Se rendre coupable directement ou indirectement quel que soit le moyen** (informatique, téléphonique, courrier…), de délits dits de presse (diffamation, injure…) ou procéder au stockage de documents proscrits par la loi (détention d'images ou de textes à caractère pédophile ou raciste…)
• **Respecter les règles de protection du droit d'auteur** en ne se rendant pas coupable de contrefaçon : > à l'occasion d'un téléchargement de données (marque, son, image, texte …) depuis un site Internet, > en faisant une copie d'un logiciel commercial pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle, > en photocopiant sans autorisation des documents protégés (articles de presse, livres, …) à des fins autres que privées.	- **Utiliser ou détourner à son profit ou celui d'un tiers** tout ou partie d'information auquel il a accès, que cela soit ou non dans le cadre de ses missions. - **Porter atteinte directement ou indirectement aux systèmes de traitement automatisés** des données, aux bases de données et aux logiciels : intrusion ou utilisation sans autorisation… ; et ce conformément aux dispositions du code pénal. - **Divulguer en dehors des obligations légales** des informations nominatives sans le consentement des personnes.

En cas de doute sur la légalité d'une opération, les utilisateurs peuvent consulter les services de documentation qui mettent à leur disposition des ouvrages et textes de lois ou consulter la règlementation de la propriété intellectuelle sur le site internet : **www.legifrance.gouv.fr**

3. Modalités d'accès aux ressources informatiques et numériques

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

La communauté de Val de Garonne Agglomération met à la disposition de ses utilisateurs, différentes ressources tel que définies au chapitre 1 selon les modalités suivantes :

- Lorsque l'utilisation d'un code identifiant/mot de passe est requis, son utilisation est strictement personnelle. Il ne peut en aucune manière être cédé, même temporairement même à un tiers (y compris un collègue).

- Tout utilisateur est responsable de l'usage des ressources du système d'information auxquelles il a accès. En tant que contributeur clé à la sécurité générale, il doit utiliser ces ressources de façon rationnelle, loyale et conforme aux obligations légales afin d'en éviter la saturation ou le détournement abusif à des fins personnelles.

La protection du patrimoine informationnel de Val de Garonne Agglomération vise avant tout à assurer sa disponibilité, son intégrité, et sa confidentialité (communication de l'information aux seules personnes habilitées). Le rôle de chacun est fondamental, dans la mesure où les seules dispositions organisationnelles et technologiques prises par VGA ne sont pas suffisantes.

La DSI, responsable de la sécurité des réseaux, est seule habilitée à diffuser toute information sur les recommandations en matière de sécurité et notamment les virus informatiques.

Toute une infrastructure invisible pour l'utilisateur est aussi maintenue en état de fonctionnement.

Elle est constituée de :

- Serveurs hébergeant les fichiers et les progiciels « métier ».
- Réseaux locaux sur les différents sites.
- Système d'interconnexion des sites.
- Dispositifs de contrôle et de lutte contre les menaces internes et externes.
- Standards téléphoniques.
- Téléphones fixes et mobiles.
- Dispositifs de sauvegarde.

En l'absence de cette infrastructure, ce sont les principales activités de l'Agglomération qui seraient paralysées, induisant une dégradation du service public et un manquement aux obligations légales.

1. AUTHENTIFICATION

L'accès aux ressources informatiques repose sur l'utilisation d'un nom de compte

(« login » ou identifiant) communiqué à l'utilisateur lors de son arrivée dans la collectivité. Un mot de passe est associé à cet identifiant de connexion.
Les moyens d'authentification sont personnels et confidentiels. Chaque utilisateur est responsable de l'utilisation qui peut être faite de ses identifiants.
Pour des raisons de sécurité évidentes, la DSI se réserve le droit de modifier à tout instant les règles de complexité des mots de passe (nombre de caractère minimum, caractères spéciaux, etc.) et la durée de vie de ces derniers (renouvellement obligatoire tous les 6 mois par exemple).

2. SECURITE DES DONNEES ET DU RESEAU

Tout utilisateur s'engage à respecter les règles suivantes :

- Usurpation d'identité: Ne pas tenter de masquer sa véritable identité ou d'usurper l'identité d'une autre personne pour accéder à ses informations.

- Respect des données d'autrui: Ne pas tenter de lire, modifier, copier ou détruire des données autres que les siennes même si celles-ci ne sont pas explicitement protégées exception faite des données diffusées dans des dossiers publics ou partagés clairement identifiés.

- Accès aux postes de travail : Ne pas laisser les ressources accessibles à des tiers en cas d'absence du poste de travail : verrouiller le poste avant de s'absenter même momentanément. En outre, il convient de rappeler que les visiteurs ne sont pas autorisés à accéder au Système d'Information de la collectivité sans accord préalable de la DSI. Les intervenants extérieurs doivent s'engager à respecter la présente charte.

- Téléchargement et installation de logiciels : Ne pas télécharger, installer, utiliser ou contourner l'utilisation d'un logiciel pour lequel la collectivité n'a pas acquis de licence. Seuls les agents de la DSI sont habilités à installer des logiciels, y compris des logiciels libres.

- Equipements étrangers : Ne pas connecter sans autorisation, à un poste ou au réseau, un équipement étranger à la collectivité et susceptible de provoquer des dysfonctionnements ou d'introduire des virus informatiques. Toute connexion d'un nouveau matériel doit se faire avec l'autorisation de la DSI.

- Virus : L'utilisateur s'engage à ne pas perturber volontairement le bon fonctionnement des systèmes informatiques et les réseaux, que ce soit par des manipulations anormales du matériel ou par l'introduction de logiciels parasites (virus, chevaux de Troie, ransomware, etc.). Des comportements inhabituels d'un logiciel ou d'un ordinateur tels que l'ouverture intempestive de fenêtres, l'activité inexpliquée du disque dur ou la dégradation importante des performances peuvent traduire la présence d'n logiciel parasite : contacter la DSI.

- Antivirus : La DSI installe sur chaque ordinateur un logiciel destiné à vous protéger des programmes malveillants. Il est absolument interdit de désinstaller cet outil ou de tenter d'en modifier le paramétrage. Le logiciel antivirus vous avertit en cas de détection de virus : vous devez en informer la DSI immédiatement.

4. Partage de ressources

Les utilisateurs disposent d'espace de stockage sur les réseaux informatiques de la collectivité : bases de données, serveurs de messagerie, serveurs de fichiers, etc. Les documents traités par les services et les données traitées par les différents progiciels sont stockés sur des serveurs accessibles via le réseau local ou des réseaux interconnectés.

L'accès à ces serveurs est limité par des droits donnés par l'administrateur à un utilisateur suite à la demande écrite de son responsable de service ou au responsable fonctionnel d'un progiciel.

Ces autorisations sont liées à un compte utilisateur nominatif.

Ces ressources étant partagées, l'utilisation abusive par un utilisateur d'espace ou de connexions pénalise l'ensemble des autres utilisateurs.

La DSI assure la sauvegarde de toutes les informations stockées sur les ressources prévues à cet effet et uniquement celles-ci. Ainsi, la sauvegarde des fichiers stockés sur le poste de travail de l'utilisateur est de la responsabilité de ce dernier. En outre, il est rappelé que la sauvegarde de fichiers professionnels sur des supports personnels ou sur des sites extérieurs à la collectivité est strictement prohibée.

Il est impératif:

- de ne conserver sur les serveurs mis à votre disposition que les données directement liées à l'activité professionnelle.
- de ne pas utiliser, même temporairement, l'infrastructure informatique de VGA pour copier transférer ou traiter des données personnelles.

Toutes les données identifiées comme privées ou personnelles sur ces espaces sont susceptibles d'être purement et simplement supprimées sans préavis.

Si des fichiers personnels devaient être stockés, ils le seront dans le répertoire « Mes documents » de son poste de travail avec la mention « perso » ou « personnel » figurant explicitement dans le nom du dossier correspondant.

5. Traçabilité des connexions

Des dispositifs de connexion gérés par la DSI conservent des traces des connexions effectuées depuis les postes de travail fixes ou mobiles.

Les informations enregistrées sont les suivantes :

- La traçabilité des connexions téléphoniques, à savoir la liste des appels (appelant, appelé, durée), sans enregistrement des contenus des appels servent principalement à des fins statistiques, leur durée de conservation est 36 mois maximum;

- La traçabilité des copieurs, à savoir la liste des volumes de copies, d'impression et de numérisation par utilisateur est de 36 mois maximum. Les comptes AD qui sont supprimés sont anonymisés et ne sont utilisés qu'à des fins statistiques ;

- Sur les serveurs d'authentification : la trace des connexions effectuées depuis le

réseau interne est enregistrée sur le modèle suivant,

- l'identifiant de l'utilisateur
- l'horodatage de l'ouverture ou de la fermeture de session
- durée de conservation : 2 mois maximum

- Sur le système de contrôle des connexions vers Internet : la trace des connexions effectuées depuis le réseau interne ou les postes mobiles est enregistrée sur le modèle suivant,
  - le nom du poste de travail,
  - l'adresse réseau du poste de travail
  - l'identifiant de l'utilisateur
  - l'adresse du serveur de destination
  - les pages Web demandées
  - l'horodatage
  - l'autorisation ou le blocage de l'accès (par exemple sites web relevant des catégories : armes, sexe, drogues, alcools, violence, terrorisme, …)
  - les raisons de l'éventuel blocage
  - durée de conservation: 36 mois maximum

- L'accès à certains locaux de la collectivité est contrôlé par des automatismes permettant ainsi de limiter les entrées de personnes étrangères aux services à certaines plages horaires. Les utilisateurs et/ou services nécessitant un accès sont alors dotés de badge permettant l'ouverture des portes en dehors des plages horaires d'ouverture au public. Il est absolument interdit de céder ou prêter son badge ou celui du service à une personne non autorisée. En outre, les agents dotés reconnaissent être informés que chaque utilisation de leur badge donne lieu à un enregistrement horodaté dans le respect de la législation en vigueur.
  La traçabilité de l'accès aux locaux est conservée par la DSI, à savoir la liste des entrées des utilisateurs en-dehors des horaires d'ouverture au public.

Ces informations pourront être communiquées à des tiers :

- pour se conformer à des obligations légales ou pour obéir à des injonctions judiciaires,
- pour protéger et défendre ses droits, notamment ses droits de propriété,
- pour protéger les intérêts des agents et des élus.

Les fichiers constitués dans le cadre de cette traçabilité font l'objet d'une déclaration auprès du COTECH RGPD pour validation. La durée maximale de conservation des données collectées est de 36 mois avant la suppression des données.

6. Règles d'utilisation de la messagerie électronique

- Ne pas ouvrir de pièce jointe d'un courriel, ou cliquer sur un lien contenu dans le message, dont on n'est pas absolument certain de la provenance et de l'innocuité.

- L'utilisation à titre professionnel de comptes de messagerie non gérés par la collectivité est strictement interdite.

- Les usages privés des listes de destinataires doivent rester exceptionnels. Les envois de mails collectifs (CNAS, Amicale, …) doivent être limités, éviter de joindre des pièces jointes et favoriser un renvoi vers l'extranet.

- En cas d'absence d'un agent, la continuité du service doit être assurée :
    - L'agent doit veiller à ce que le service puisse accéder aux documents, logiciels et dossiers indispensables à l'activité (transfert de courriel ou message d'absence, mise à disposition des documents dans un dossier partagé, etc.,) à l'exclusion de toute communication de mots de passe personnels.
    - En cas d'absence imprévue, la direction pourra demander à la DSI l'accès à l'espace de travail de l'agent ou la transmission d'un message électronique à caractère exclusivement professionnel et identifié comme tel par son objet et/ou son expéditeur. L'agent est informé dès que possible de la liste des messages transférés.
    - En cas d'absence prolongée d'un agent (longue maladie), la Direction, peut demander à la DSI la mise en place d'un message d'absence. L'agent prendra les dispositions nécessaires pour ne plus recevoir de messages à caractère personnel sur sa messagerie professionnelle.
    - En cas de départ définitif de la collectivité, le successeur récupère les documents de travail. La DSI pourra mettre en place un message de départ de la collectivité. Les comptes et les données personnelles de l'utilisateur sont, en tout état de cause, supprimés dans un délai maximum d'un mois après son départ.

7. Logiciels métier et télé services

Sont ici qualifiés de « logiciels métier » les logiciels de gestion accessibles en ligne, à titre d'exemple Système d'information géographique, Gestion de relation citoyen, Gestion de projets, Portail famille, Observatoires, Logiciels : SEDIT, PostOffice, Atal, ECongés, HelpDesk (liste non limitative).

Chaque utilisateur doit être authentifié pour accéder au logiciel métier avec les droits qui lui ont été attribués par l'administrateur du logiciel métier. L'authentification se fait via un compte utilisateur nominatif, comportant un identifiant et un mot de passe.

L'utilisateur doit respecter les règles d'usage du logiciel métier pour lequel des droits lui ont été attribués.

L'utilisateur n'est pas autorisé à utiliser un logiciel métier non validé par son chef de service pour traiter des données de la collectivité.

8. Protection des données personnelles

Dans le cadre de réglementation sur la protection des données personnelles (RGPD), il revient aux agents responsables de traitements ou créateurs de fichiers contenant des données personnelles d'en faire la déclaration auprès du délégué à la protection des données (DPO) et du Relais Informatique et libertés (RIL) de la collectivité avant toute utilisation : dpo@vg-agglo.com

Pour aider l'agent dans cette tâche un référent RGPD est identifié par service ou par pôle. Sa mission consiste dans un premier temps à identifier les nouveaux traitements au sein des projets métiers afin qu'ils puissent être qualifiés par le DPO et par le RIL puis à remonter les informations permettant d'effectuer le suivi des traitements.

Le référent RGPD est également un relais entre son service d'une part, le DPO et le RIL d'autre part:

- relais descendant, il diffuse dans son service les bonnes pratiques et les procédures à respecter.

- relais ascendant, il remonte au DPO et au RIL les questions, les difficultés rencontrées ou les spécificités locales (exemple: réglementation spécifique à un métier, contraintes métier en conflit avec les exigences Informatique et liberté, etc.).

Dans le cas d'une donnée sensible, l'utilisateur doit faire une déclaration auprès de son référent RGPD pour obtenir la validation du COTECH RGPD (Comité Technique du Règlement Général de la Protection des Données) de VGA animé et coordonné par le service numérique de VGA.

9. Déconnexion

VGA s'engage à contribuer à une articulation optimale entre la vie personnelle et la vie professionnelle de chaque collaborateur pour l'utilisation des technologies actuelles et futures.

Les outils numériques (ordinateurs, téléphones et/ou tout support multimédia rentrant dans cette catégorie) mis à disposition des agents par VGA à des fins professionnelles sont susceptibles d'être utilisés en dehors des horaires de travail. VGA rappelle à ses agents qu'il n'existe pas d'obligation liée à l'utilisation des outils hors des horaires indiqués dans leurs contrats de travail. Si l'utilisation des outils numériques peut être effectuée hors des horaires de travail afin d'optimiser l'accomplissement de tâches nécessitant une actualisation dans les meilleurs délais, VGA recommande à l'ensemble de ses agents de veiller à ne pas faire une utilisation qui porterait une atteinte manifeste à l'équilibre entre leur vie personnelle et leur vie professionnelle.

Concernant les agents en situation de télétravail, ces derniers pourront annuellement analyser avec la Direction et le service des Ressources Humaines, outre les conditions d'activité de l'emploi concerné, les plages horaires durant lesquelles VGA pourra habituellement prendre contact avec le collaborateur.

10. Télétravail

L'Article 133 de la loi n° 2012-347 du 12 mars 2012 a consacré la possibilité pour les agents publics (fonctionnaires ou non) d'exercer leurs fonctions dans le cadre du télétravail. Le décret n°2016-151 du 11 février 2016 reprend peu ou prou la définition du télétravail fixée à l'article L.1222-9 du Code du travail, qu'il définit comme toute forme d'organisation du travail, dans laquelle les fonctions qui auraient pu être exercées par un agent dans les locaux de son employeur sont réalisées hors de ces locaux de façon régulière et volontaire, en utilisant les technologies de l'information et de la communication.

Afin de faciliter l'accès des agents de VGA qui le souhaitent au télétravail, un document spécifique au télétravail définira ses modalités de mise en œuvre :

- Les activités éligibles au télétravail,
- Le temps possible de télétravail,
- la liste et la localisation des locaux professionnels éventuellement mis à disposition par l'administration pour l'exercice des fonctions en télétravail,
- les règles à respecter en matière de sécurité des systèmes d'information et de protection des données , de temps de travail, de sécurité et de protection de la santé.
- les modalités de contrôle et de comptabilisation du temps de travail ;
- les modalités de prise en charge, par l'employeur, des coûts découlant directement de **l'**exercice du télétravail, notamment ceux des matériels, logiciels, abonnements, communications et outils ainsi que de la maintenance de ceux-ci,
- les modalités de formation aux équipements et outils nécessaires à l'exercice du télétravail.

11. Téléformation

Afin de faciliter l'accès à des modules de télé formation dans le cadre du plan de formation professionnelle des agents, un document spécifique à la téléformation définira ses modalités de mise en œuvre :

- L'usage du matériel sur son lieu professionnel
- L'usage sur un tiers lieux
- L'usage en télé travail

12. Réseaux sociaux

Les medias sociaux regroupent les différentes activités qui intègrent l'interaction sociale et la création de contenu. Ces outils prennent de plus en plus de place dans nos communications. Les collectivités locales et leurs établissements sont confrontés aux mutations qu'entraînent les outils numériques dans nos modes de communication.

Les plateformes sociales sont des véritables espaces publics, visibles et consultables par tous. Tout le monde peut propager vos idées en republiant un contenu écrit, vidéo ou audio instantanément. Par ailleurs, l'agent est impliqué personnellement sur tout ce que qu'il publie ou retransmet (partage, ''like'',retweet, commentaire, etc..).

La facilité d'accès, l'illusion d'anonymat sur les réseaux sociaux, ne doivent pas faire

oublier aux agents l'exercice de leurs obligations, qui continuent à s'appliquer même en dehors du cadre professionnel. Aussi bien sur les réseaux gérés par l'Agglomération que sur ses réseaux personnels, chaque agent demeure soumis aux obligations de réserve, de discrétion et de secret professionnel. A ce titre, il leur est demandé notamment de faire preuve de mesure dans leurs propos afin de ne pas porter atteinte à l'image ou à la considération de VGA.

L'usage des réseaux sociaux durant le temps de travail doit rester limité à un usage professionnel.

Pour tous les réseaux sociaux gérés par l'Agglomération, Il est notamment interdit de :

- promouvoir des activités illégales sous quelques formes que ce soit, notamment la copie ou la distribution non autorisées 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, le négationnisme et le terrorisme.
- publier des contenus contrevenant aux droits d'autrui, incitant aux crimes, aux délits et à 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.
- publier une image ou une photo sans mentionner son auteur et d'avoir obtenu son accord préalable. Il faut également l'accord des personnes qui sont photographiées.

Les informations postées par les utilisateurs sont indexées par les moteurs de recherche. Elles laissent des traces durables qui peuvent suivre un utilisateur tout au long de sa vie. Il est donc nécessaire de s'exprimer en toute connaissance des sujets traités.

13. Règles minimales de courtoisie et de respect d'autrui

Il convient de faire preuve de la plus grande courtoisie à l'égard de ses interlocuteurs dans les échanges électroniques et téléphoniques.

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

Messages non sollicités: Veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter l'encombrement inutile de la messagerie et une

dégradation des temps de réponse. Toujours dans l'optique d'éviter une saturation des réseaux, les utilisateurs sont invités à limiter leur consentement préalable à recevoir un message de type commercial, newsletter, abonnement, etc., et de ne s'abonner qu'à un nombre limité de listes de diffusion notamment si elles ne relèvent pas du cadre strictement professionnel.

Emploi de la langue française : Eviter l'emploi de termes en langue étrangère dans tous types de communication. Lorsque des termes français de même sens existent, leur emploi est vivement conseillé.

Photographies, droits à l'image : L'image d'une personne ne peut être utilisée sans son consentement écrit. D'une manière générale, les photos que les agents sont amenés à prendre dans l'exercice de leurs fonctions ne doivent pas comporter de personnes, plaques d'immatriculation, etc. Les photos prises dans le cadre des activités de la collectivité ou dans ses locaux ne peuvent pas être utilisées à des fins personnelles et sont interdites à la diffusion externe sans le consentement de la direction. Cette recommandation s'applique aux enregistrements sonores et vidéo. Les formulaires d'autorisation sont disponibles sur le serveur dans le répertoire photothèque.

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

14. Spécificités applicables aux instances représentatives du personnel

Les instances représentatives du personnel utilisent dans le cadre de leur mandat, les outils de communication électronique qui leur sont attribués pour l'exercice de leur activité. Ces outils répondent aux mêmes règles d'usage que tout autre outil générique au sein de VGA, garantissant déontologie et de confidentialité.

Dans le respect de la liberté syndicale d'une part, de la liberté de choix des agents de recevoir ou pas une information par messagerie électronique, d'autre part, tout répondant aux les exigences de bon fonctionnement du réseau informatique, une liste de diffusion spécifique est mise en place pour chacune des organisations syndicales de VGA. Ces dernières disposent d'une adresse mail spécifique pour leur permettre d'échanger selon leurs besoins et de recevoir des informations de la DG ou de la DRH.

En matière d'usage, il n'est pas conseillé d'utiliser les envois en masse avec ou sans pièce jointe mais plutôt de se servir des panneaux d'affichages mis à leur disposition. *Est-il*

possible d'envisager que les représentants du personnel disposent d'un espace d'affichage sur l'Intranet ?

La confidentialité des échanges électroniques entre le personnel et leurs représentants ou les organisations syndicales est garantie. VGA s'engage à n'exercer aucun contrôle sur les listes de diffusion, garantissant ainsi toute impossibilité d'utilisation détournée, notamment sur l'opinion d'un agent à l'égard d'une organisation syndicale voire son appartenance, ou sur le choix opéré, d'accepter ou non de recevoir des messages à caractère syndical.
Le Comité technique (CT) sera consulté pour avis préalablement à la décision de mise en œuvre de la présente charte dans la collectivité.

15. Mesures prises en cas d'infraction / gestion des abus

Une procédure disciplinaire et/ ou pénale, pouvant aller jusqu'au licenciement pour faute grave, en fonction de la gravité et/ou des conséquences des faits sur le préjudice subi par l'employeur, pourra être engagée envers l'utilisateur suite à une utilisation non conforme à cette charte ou des législations en vigueur.

La Direction se réserve le droit, en cas d'une utilisation contraire à cette charte, d'interdire l'utilisation d'Internet et/ou de la Messagerie à titre privé à une personne ou à l'ensemble des utilisateurs.

16. Evolution, modification

Les modifications et extensions prévues du système d'information et de communication électronique qui affectent de manière perceptible l'objet de cette présente charte seront communiquées aux délégués du personnel et au Délégué à la Protection des Données.

La Charte des usages numériques et du système d'information sera modifiée en conséquence et, le cas échéant, après consultation et information aux délégués du personnel, et sera communiquée au personnel de VGA.

17. Responsabilités

En cas du non-respect de la présente charte ou de la législation en vigueur, outre la mise en œuvre de sanctions disciplinaires à l'encontre des utilisateurs, l'organisme se réserve le droit d'appeler en garantie la personne pour les dommages et intérêts qu'elle aura dû éventuellement régler à un tiers en raison des agissements de cette dernière.

L'utilisateur est donc informé qu'il peut engager sa responsabilité civile et/ou pénale.

18. Disposition finale

L'accès aux ressources informatiques ne pourra se faire qu'après acceptation des modalités précisées dans la charte. La DSI met en place toutes les mesures techniques nécessaires à son application et au contrôle de son exécution.

La charte des administrateurs s'adresse aux personnes ayant accès au système de gestion et d'administration du système d'information et des services numériques de l'agglomération

Cette charte fera l'objet d'une validation en conseil communautaire et sera annexée au

règlement intérieur de la collectivité.

Cette charte annule et remplace la précédente charte de bon usage.

La présente charte est accessible sur l'extranet des agents.