
Charte du bon usage des ressources du système d'information et de communication Internet, messagerie, téléphonie, impressions.

SOMMAIRE

- Préambule

- 1 - Champ d'application

- 2 – Autorisation d'accès

- 3 – Règles d'utilisation
 - 3.1 Téléphonie fixe et mobile
 - 3.2 Informatique et internet
 - 3.3 Messagerie
 - 3.4 Impressions

- 4 – Matériel informatique
 - 4.1 Equipement informatique
 - 4.2 Entretien
 - 4.3 Renouvellement des équipements informatiques
 - 4.4 Règles de sécurité

- 5– Protection des données personnelles

- 6 – Contrôle de l'usage

- 7 – Télétravail

- 8 – Dispositions légales

- 9 – Sanctions applicables

Préambule

Les nouvelles technologies permettent aujourd'hui aux agents de bénéficier d'importants moyens d'échanges et d'informations.

Le WEB (la toile) permet de consulter des informations d'ordre juridique, économique, technique, des actualités mais également de participer à des forums de discussions professionnels.

Les sites d'informations professionnelles spécialisées, mais aussi ceux des organismes publics, des collectivités locales, tout comme ceux des associations et des entreprises, constituent des sources d'informations considérables et accessibles très rapidement.

Par ailleurs, notre système de messagerie permet l'échange de messages, de documents, entre les agents disposant d'une adresse électronique au sein de notre collectivité (réseau intranet) mais aussi avec l'extérieur via le réseau Internet – e-mail.

Cette charte a pour objet :

- de préciser la responsabilité des utilisateurs, en accord avec la législation en vigueur, afin d'instaurer un usage correct des ressources informatiques et des services internet avec des règles minimales de courtoisie et de respect d'autrui, cela dans le respect du cadre général des droits et obligations des agents publics ;
- d'informer les utilisateurs de leurs devoirs et de leurs droits liés au respect de la vie privée.

1 – Champ d'application

La présente charte s'applique à l'ensemble des agents, tous statuts confondus, ainsi qu'aux apprentis et aux stagiaires reçus dans les services, qui accèdent aux systèmes d'informations et de communications de la Communauté d'Agglomération Val Paris.

La présente charte s'applique à l'ensemble des ressources de communication et d'information de la Communauté d'Agglomération Val Paris :

- Logiciels métiers, bureautiques, messagerie, Internet ;
- PC fixes, PC portables, périphériques notamment imprimantes, clés USB, scanners...etc. ;
- Téléphones fixes, mobiles ;
- Télécopies, photocopieurs ;
- Appareils photo numériques...etc.

2 – Autorisation d'accès

Le droit d'accès au système d'information et de communication est personnel et incessible.

L'utilisateur est responsable de l'utilisation des ressources informatiques (locales ou distantes) effectuées à partir de son droit d'accès.

Dans le respect de la réglementation en matière de secret de la correspondance, il s'engage cependant à une utilisation essentiellement professionnelle, rationnelle et loyale afin d'en éviter la saturation.

Le droit d'accès et d'usage est temporaire et disparaît dès que son utilisateur ne remplit plus les conditions qui lui ont autorisé l'accès. Cette mesure est valable pour l'ensemble des outils de service mis à disposition de l'agent. Ces outils doivent impérativement être restitués à la collectivité en cas d'absence prolongée ainsi que, bien entendu, à la fin de son engagement.

3 – Règles d'utilisation

3.1 Téléphonie fixe et mobile

- L'utilisateur d'un terminal mobile respecte les limitations du forfait fourni ;
- Il est interdit d'utiliser la carte SIM professionnelle sur un autre terminal mobile que celui fourni ;
- Afin de limiter l'empreinte carbone, les agents sont autorisés à utiliser leur carte SIM personnelle dans leur terminal professionnel si ce dernier est dual-SIM.

3.2 Informatique/Internet

- La navigation sur des sites déviants (pornographie, racisme...etc.) est interdite. Tout message électronique ou téléphonique, de nature diffamatoire, discriminatoire (raciste, sexiste) ou d'incitation à la violence, tombe sous le coup de la loi pénale ;
- L'utilisateur doit assurer la confidentialité des données qu'il détient et n'accéder qu'aux informations et documents qui lui sont propres, publics ou partagés. Il ne doit modifier ou supprimer que les seules données dont la responsabilité lui est confiée ;
- Un usage personnel ponctuel et raisonnable des ressources du système d'information et de communication dans le cadre des nécessités de la vie courante et familiale est toléré, à l'exception des réseaux sociaux, des jeux et paris en ligne et du téléchargement de médias, dans la limite des accès autorisés, dès lors qu'il ne se fait pas au détriment du travail de l'agent et qu'il n'est pas susceptible d'affecter le bon fonctionnement de l'outil ou de mettre en cause les intérêts et/ou la réputation de la Communauté d'Agglomération Val Parisis. Ainsi, l'utilisation privée doit être non lucrative et limitée tant dans sa fréquence que dans sa durée ;
- Souveraineté des données : le partage de documents via des sites tiers souvent situés à l'étranger, non soumis aux lois françaises et européennes, est proscrit, comme WeTransfer ou Google Drive. Pour le partage de fichiers, il est possible d'utiliser cloud.valparisis.fr ou la plateforme share.valparisis.fr, pour les autres besoins, n'hésitez pas à contacter le service informatique qui vous accompagnera ;
- La diffusion de son adresse e-mail par l'agent sur des sites webs externes ne doit se limiter qu'à des sites professionnels afin de limiter les risques de tentatives d'intrusion, la contamination par des virus ou un « cheval de Troie ». La diffusion de l'adresse e-mail à des sociétés commerciales doit être strictement limitée car celle-ci peut être source d'envoi de nombreux messages plus ou moins volumineux et souvent à caractère essentiellement publicitaire ;
- Chaque utilisateur doit enregistrer ses documents personnels en créant un dossier personnel facilement identifiable en local sur son ordinateur (par exemple : « Dossier personnel »). Ce sous dossier est considéré comme un dossier de vie privée ;
- L'achat, l'installation, le téléchargement ou l'utilisation de tout logiciel sont de la compétence exclusive du service Informatique ;
- Il est interdit de modifier le matériel (mémoire, disques durs, lecteurs divers CD et DVD) ainsi que les périphériques (son, imprimantes, scanners...etc.) ou d'introduire du matériel personnel ;
- Les disques durs des serveurs ne servent qu'à stocker des documents de travail. Les médias personnels (photos, fichiers musicaux...) n'y sont pas les bienvenus. Ils peuvent par contre être hébergés directement sur les ordinateurs sous la responsabilité de leur propriétaire ;

- Le service informatique ne garantit pas la récupération des documents de travail stockés directement sur les ordinateurs, en cas de défaut du disque dur. Il appartient à l'utilisateur d'enregistrer ses fichiers sur les lecteurs réseau prévus à cet effet.
- Les sessions utilisateurs sont automatiquement verrouillées au bout de 30 minutes d'inactivité.

3.3 Messagerie

- L'utilisateur doit faire usage des services Internet et de la messagerie électronique dans le cadre de ses activités professionnelles ;
- L'utilisateur doit obtenir l'aval du responsable hiérarchique préalablement à toute transmission d'information engageant d'une manière quelconque la Communauté d'Agglomération Val Parisis ;
- L'utilisateur consulte sa boîte mails quotidiennement ;
- L'utilisation des groupes de destinataires (chefs de service, etc.) est exclusivement réservée au cadre professionnel, d'une part, et pour la diffusion d'une information d'intérêt général d'autre part. Ces listes doivent être utilisées à bon escient pour éviter de perturber le bon fonctionnement du réseau ;
- Avant l'envoi d'un message interne, il est conseillé de vérifier le nom des destinataires afin d'éviter les erreurs ou les envois à des homonymes ;
- Ce système de communication ne dispense pas d'utiliser la voie hiérarchique traditionnelle ;
- Toute correspondance d'ordre personnel doit préciser qu'elle est personnelle dans l'objet du message.
- En cas d'absence prolongée, il est nécessaire de renseigner le gestionnaire d'absence afin que les correspondants soient informés et puissent avoir les coordonnées d'un autre interlocuteur.
- L'utilisateur gère le stockage de sa boîte aux lettres. En cas de saturation, il doit trier et/ou archiver ses messages anciens, obsolètes ou trop volumineux.
- Lors du départ de l'agent de la collectivité, celui-ci est invité à nettoyer sa messagerie et notamment à supprimer tous les courriels à caractère personnel. Il doit également activer un message d'absence du bureau en communiquant les coordonnées d'une autre personne à contacter en accord avec son responsable. L'adresse de l'agent ainsi que les emails restants seront supprimés un mois après son départ. Les courriels restant dans la messagerie seront susceptibles d'être consultés pour le bon fonctionnement du service pendant cette période. L'adresse pourra également être redirigée sur l'adresse d'un autre agent afin de ne pas perdre les messages professionnels qui pourraient être adressés à la Communauté d'Agglomération et de pouvoir répondre aux interlocuteurs.

3.4 Impressions

- L'utilisateur s'engage à limiter sa consommation de papier, en n'imprimant que le strict nécessaire.
- L'impression noir et blanc est la norme, l'usage de la couleur doit être limité et justifié.
- Pour les documents volumineux, privilégiez le recto-verso, voir l'impression de miniatures (4 pages par feuille).

4 – Matériel informatique

4.1 Equipement informatique

La collectivité fournit aux agents les outils nécessaires à l'accomplissement de leurs missions. Les équipements informatiques mis à disposition peuvent comprendre :

- Ordinateur fixe ou portable
- Périphériques, écran, station d'accueil, clavier, souris, certificat, carte SD
- Smartphone, tablette
- Photocopieur
- Appareil photo, caméra

4.2 Entretien

Les agents s'engagent à prendre soin du matériel qui leur a été confié pendant la durée de leur mission. Leur responsabilité pourra être engagée en cas de négligence avérée.

4.3 Renouvellement des équipements informatiques

Soucieuse de limiter son empreinte carbone, la collectivité ne renouvelle plus systématiquement le matériel à échéance régulière. Il n'a pas de renouvellement tant que le matériel est fonctionnel ou obsolète. Seule la DSI peut juger de l'opportunité du renouvellement anticipé d'un équipement.

4.4 Règles de sécurité

L'utilisateur s'engage à :

- Choisir des mots de passe ou des phrases de passe sûrs qui ne devront pas être communiqués à des tiers (au minimum 12 caractères, majuscules, minuscules, chiffres, caractères spéciaux ?!*@*...);
- Utiliser les moyens mis à sa disposition pour assurer la sécurisation de l'accès à son poste de travail, le mode veille avec mot de passe pouvant s'avérer suffisant dans la majorité des cas. Par ailleurs, à la fin de sa journée de travail, l'utilisateur doit éteindre son poste informatique (ordinateur et écran) ;
- L'utilisateur doit enregistrer tout document de travail sur l'espace réseau dédié à son service afin de bénéficier des sauvegardes journalières et permettre l'accès aux documents à sa hiérarchie. Le service informatique ne garantit pas la récupération des documents de travail stockés directement sur les ordinateurs, en cas de défaut du disque dur;
- L'utilisateur est tenu de signaler, dans les plus brefs délais, au service Informatique, tout incident de sécurité ou de fonctionnement (apparition de virus, tentative d'intrusion ou intrusion...etc.) qu'il serait amené à observer.

5 – Protection des données personnelles

Les utilisateurs doivent respecter la réglementation relative à la protection des données personnelles, en particulier la loi Informatique et libertés et le Règlement Général sur la Protection des Données (RGPD).

- Les nouveaux traitements de données personnelles effectués par l'utilisateur dans le cadre de ses fonctions doivent obligatoirement être déclarés auprès du Délégué à la protection des données (DPO). Une donnée personnelle est une information qui permet d'identifier directement ou indirectement une personne.
- Les données personnelles contenues dans des fichiers ou logiciels ne peuvent être conservées indéfiniment.

- Selon les traitements, les personnes dont les données sont traitées doivent être informées :
 - Des données collectées,
 - De la finalité de la collecte,
 - Des destinataires internes et externes
 - De la durée de conservation,
 - De leurs droits

Pour vous aider, vous pouvez contacter le Délégué à la protection des données à dpd@valparisis.fr. En cas de violation de données personnelles survenue dans votre service, chaque utilisateur doit en informer le DPO ou la DSI sous 48 heures. Une violation de données peut être une cyberattaque, un piratage, un mail frauduleux, un fichier supprimé par inadvertance, un support de stockage perdu (clé usb, disque dur) etc.

Une fiche pratique avec des exemples est disponible sur l'espace commun

6 – Contrôle de l'usage

Pour des nécessités de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent être analysés et contrôlés, de manière automatique ou manuelle, dans le respect de la législation, notamment de la loi du 6 janvier 1978 relative à l'informatique et les libertés.

Pour la téléphonie fixe et mobile, le contrôle mis en œuvre porte sur les éléments suivants :

- Les durées d'appels,
- Les coûts par ligne,
- Les hors-forfaits.

Pour les services Internet, le contrôle mis en œuvre porte sur les éléments suivants :

- Les durées de connexion,
- Les sites visités.

Pour la messagerie électronique, le contrôle mis en œuvre porte sur les éléments suivants :

- Le volume des messages échangés ;
- La taille des messages échangés ;
- Le format des pièces jointes.

Pour les impressions, le contrôle mis en œuvre porte sur les éléments suivants :

- Les volumes d'impressions noir et couleur (de façon globale/ par service/par utilisateur) ;

7 – Télétravail

Le télétravail est autorisé dans le cadre défini par les ressources humaines. Seul le matériel fourni par l'agglomération (ordinateur, smartphone) peut être utilisé pour se connecter au système d'informatique de la collectivité.

Les agents qui ne sont pas dotés d'un ordinateur portable peuvent en emprunter un à l'accueil dans le pool dédié à cet effet. Les réservations sur GLPI sont obligatoires.

Les agents en télétravail doivent veiller à réaliser le renvoi de leur téléphone fixe vers leur téléphone mobile ou le softphone Teams.

Les dispositions ci-dessus peuvent varier en fonction des contraintes sanitaires.

8 – Dispositions légales

Il est rappelé que toute personne sur le sol français doit respecter les législations françaises et européennes, en particulier dans le domaine de la sécurité informatique et de la protection des logiciels :

- Loi du 6 Janvier 1978 dite informatique et libertés,
- Règlement général sur la protection des données du 27 avril 2016
- Loi du 30 Septembre 1986 relative à la liberté de communication,
- Législation relative à la fraude informatique (et notamment les articles 323-1 à 323-7 du code Pénal),
- Législation relative à la propriété intellectuelle,
- Législation en matière de cryptologie,
- Code pénal, notamment les articles 226-16 à 226-24 sur les atteintes aux droits de la personne résultat des fichiers ou des traitements informatiques
- Code général de la fonction publique, notamment sur les droits et obligations des fonctionnaires (article L121-5 et suivants)

9 – Sanctions applicables

La loi, les textes réglementaires et cette charte définissent les droits et obligations des personnes utilisant les ressources informatiques et les services internet.

L'utilisateur qui contreviendrait aux règles précédemment définies s'expose à des sanctions disciplinaires ainsi qu'aux poursuites pénales prévues par la réglementation en vigueur.

Notifié aux agents par le biais du coffre-fort numérique.