Stratégie numérique 2022 – 25, Antenne Région Valais romand, Mise en œuvre | Bonnes pratiques

**Annexe I.1: Charte utilisateurs et gestion matérielle des ressources informatiques**

**I : Charte utilisateurs***Les prestataires IT de la commune restent les interlocuteurs de référence pour cette thématique.
Cette fiche doit être considérée comme indicative et n’est en aucun cas exhaustive.*

**INFORMATIQUE & TELEPHONIE**

La charte utilisateurs permet non seulement de définir les conditions d’utilisation des ressources informatiques,
de téléphonie et d’internet, mais aussi de **responsabiliser** les salariés de la commune vis-à-vis de la sécurité
numérique et de la confidentialité des données.

**Modèle de Charte utilisateurs**

**Art. 1 GÉNÉRALITÉS**

1.1.

Sauf mention spécifique, toute dénomination de personne, de statut ou de fonction se rapporte aux personnes des deux sexes.

1.2.

Le bien-être et la santé du collaborateur restent une priorité. Dans tous les cas, le bon sens doit primer.

1.3.

Ce règlement s’applique à tout le personnel. Il fait partie intégrante du contrat de travail.

**Art. 2 BUT**

2.1.

Le but du présent règlement est de définir les droits et les devoirs des utilisateurs à propos des moyens de communication (internet, messagerie électronique, téléphonie) et des postes de travail et autres outils informatiques mis à leur disposition dans le cadre professionnel, de prévenir une utilisation abusive de ces derniers et de régler les conséquences d’éventuels abus.

**Art. 3 RESPONSABILITÉS**

3.1.

L’exécutif communal est responsable de la sécurité informatique et chargé de l’application de ces directives et de ces contrôles. Il peut également nommer une personne responsable de la sécurité informatique et de l’application de ces directives.

**Art. 4 UTILISATION**

4.1. Poste de travail et stockage des données

4.1.1

Le poste de travail est un élément constitutif du système informatique de la commune. La modification de son contenu et/ou un usage inapproprié peuvent avoir des effets sur le fonctionnement global de l’environnement informatique. Le poste de travail doit être utilisé pour accomplir des tâches professionnelles. Chaque utilisateur est responsable du matériel mis à sa disposition et de l’utilisation des données auxquelles il a accès selon le présent règlement.

4.1.2

Aucune donnée privée n’est autorisée sur le réseau. En aucun cas, la commune ne pourra être tenue responsable de la sauvegarde et de la perte de ces données.

4.1.3

Une utilisation privée des applications installées sur le poste de travail est admise exceptionnellement, en dehors du temps de travail, dans la mesure où elle ne constitue pas un abus, notamment qu’elle ne surcharge pas l’infrastructure informatique (stockage ou transfert de fichiers) et ne viole pas le devoir de fidélité et de diligence du collaborateur. Des contrôles peuvent être effectués par des personnes habilitées.

4.1.4

Il est notamment interdit de :

- Modifier la configuration matérielle du poste de travail en retirant des composants ou en installant de nouveaux ;

- Modifier la configuration logicielle du poste de travail en retirant des programmes ou en installant des programmes téléchargés depuis internet ou reçus par courrier électronique ou en provenance de toute autre source ;

- Réaliser des développements informatiques sans autorisation.

4.1.5

Les modifications effectuées en violation du chiffre 4.1.4 ci-dessus seront supprimées sans préavis. Dans le cadre de ses activités professionnelles, chaque collaborateur a accès à de nombreuses données confidentielles qu’il s’interdit de rendre accessible et/ou de diffuser par quelques moyens que ce soit à toute autre personne. Cette obligation de confidentialité dépasse la durée du contrat de travail et reste intacte même après la fin des rapports de travail.

4.1.6

Le collaborateur ne consulte, ni ne stocke ou ne diffuse des informations qui, sous quelque forme que ce soit, constituent notamment une participation à un acte illicite ou qui, en particulier, portent atteinte à la dignité de la personne, présentent un caractère pornographique, incitent à la haine raciale ou constituent une apologie du crime ou de la violence.

4.1.7

Le collaborateur reçoit un identifiant et un mot de passe qui lui sont propres et qui ne doivent être communiqués à quiconque. Ils correspondent à une signature informatique et engagent la seule responsabilité de son détenteur.

4.1.8

Le collaborateur s’engage à ne pas désactiver les protections.

4.1.9

De manière générale, le collaborateur stocke ses données sur les serveurs prévus à cet effet. Il est tenu de les épurer régulièrement.

4.1.10

Le collaborateur verrouille son poste de travail lorsqu’il quitte sa place de travail. En cas d’absence prolongée (plus d’une heure), le collaborateur quitte sa session. A la fin de la journée de travail, il éteint son poste de travail.

4.2. Portables, matériel informatique mis à disposition du personnel

4.2.1

Chaque collaborateur qui reçoit un ordinateur portable avec différents accessoires informatiques en est responsable. Ce matériel reste propriété de l’employeur.

4.2.2

Ce matériel sert aussi pour les séances à l’extérieur et est sous la responsabilité du collaborateur qui en prend soin et signale tout dégât ou problèmes rencontrés. Son usage est réservé pour des activités professionnelles uniquement et il est strictement interdit d’y télécharger des programmes ou d’en laisser libre accès à des tiers non-collaborateurs de la commune. En cas de vol ou de perte avertissez immédiatement le service informatique.

4.2.3

Aucune donnée déposée sur ce portable n’est sauvegardée et ces appareils peuvent être régulièrement repris pour des raisons de maintenance. L’employeur ne peut être tenu pour responsable de la perte de données suite à cette opération.

4.2.4

Ces portables sont équipés de logiciels permettant l’accès à distance sur les serveurs de la commune. La connexion ne peut être obtenue que sur demande auprès de la hiérarchie ou des ressources humaines, et pour une période définie. Cet accès doit absolument être utilisé de manière restrictive, car il ouvre la porte aux données internes de la commune et ne doit pas être laissé sans surveillance (verrouillage de la session en cas d’éloignement du poste). Il est fortement recommandé d'activer une double authentification pour les périphériques externes qui doivent accéder au réseau communal. Le collaborateur qui doit effectuer du télétravail doit accepter d'installer sur son téléphone portable les applications nécessaires pour la double-authentification.

4.2.5

L’utilisation abusive de ce matériel, la perte ou la délégation à des tiers de son usage est considérée comme faute professionnelle grave et passible de sanctions.

4.3. Informatique de gestion

4.3.1

Toutes les données sont à traiter avec confidentialité. Toutes divulgations à des tiers sont proscrites à l'exception du besoin d'en connaître.

4.3.2

L’extraction de données des fichiers à usage autre qu’interne ou strictement professionnel est interdite.

4.4. Internet

4.4.1

Internet doit être utilisé pour la recherche et la diffusion d’informations à but professionnel.

4.4.2

Une utilisation privée est admise en dehors du temps de travail, dans la mesure où elle ne constitue pas un abus, notamment qu’elle ne surcharge pas l’infrastructure informatique (stockage ou transfert de fichiers) ni ne viole le devoir de fidélité et de diligence du collaborateur mais aussi que son utilisation ne constitue pas un dégât d'image pour la commune.

4.4.3

L’employeur se réserve le droit de bloquer l’accès à certaines catégories de sites internet, notamment :

- Sites de transactions financières (notamment les sites boursiers) ou ceux payants ;

- Sites de jeux et de paris ;

- Sites à caractère érotique, violent, raciste ou contraire aux mœurs de quelque manière que ce soit.

4.4.4

Le collaborateur s’engage à ne pas copier illégalement des logiciels, de la musique ou des films, protégés par un « copyright », à ne pas diffuser les informations appartenant à des tiers sans leur autorisation. Il s’engage à mentionner ses sources lors de l’utilisation d’informations.

4.5. Réseaux sociaux

4.5.1

Le collaborateur est invité à relayer et promouvoir les activités de la commune au travers
de son activité sur les réseaux sociaux.

4.5.2

Le collaborateur doit en toute circonstance avoir sur les réseaux sociaux un comportement digne et en aucun cas porter atteinte à l’image et à la réputation de la commune ni de ses collaborateurs sous peine de sanctions.

4.6. Messagerie électronique

4.6.1

Messagerie professionnelle

L’utilisation du courrier électronique comme instrument de communication est réservée aux besoins professionnels. Une utilisation privée est admise à titre exceptionnel, dans la mesure où elle ne constitue pas un abus, notamment qu’elle ne surcharge pas l’infrastructure informatique (stockage ou transfert de fichiers) et qu’elle ne viole pas le devoir de fidélité et de diligence du collaborateur.

4.6.2

Messagerie privée (gmail, hotmail, etc.)

L’utilisation d’une messagerie privée, dont l’adresse est autre que utilisateur@commune.ch est interdite sauf si des contraintes techniques l’exigent. Il ne faut pas échanger des courriels professionnels depuis sa messagerie privée.

4.6.3

L’utilisation de fonctionnalités spéciales pour la messagerie est réservée exclusivement à des buts professionnels. Le collaborateur s’engage notamment à ne pas contribuer à la propagation de chaînes de distribution.

4.6.4

En cas d’absence ou de vacances, le collaborateur prend les mesures nécessaires pour assurer un suivi de ses courriers électroniques professionnels. Il active un message d’absence à l’intention des contacts externes et de ses collègues. Chaque collaborateur veille à partager avec tous ses collègues (en lecture) son agenda électronique.

4.6.5

Les fichiers attachés aux mails reçus doivent faire l’objet d’une attention particulière, notamment les extensions : .exe, .com, .bat, .xlm, .vbs, .vb. En cas de doute, il prend contact avec le support informatique.

4.6.6

Le collaborateur s’engage à ne pas diffuser des informations qui peuvent porter atteinte à la réputation de la commune.

4.6.7

Le collaborateur est rendu attentif au fait qu’un courrier électronique peut se transmettre très rapidement et qu’il doit donc être très prudent avec les informations qu’il véhicule, ceci spécialement pour des fichiers attachés à caractère confidentiel.

4.6.8

Si un collaborateur reçoit un courrier électronique à caractère violent, raciste ou pornographique, il doit avertir rapidement le supérieur. Ce dernier prendra les mesures qui s’imposent.

4.6.9

En cas d'inscription sur un site, l'adresse courriel du collaborateur peut être utilisée mais il est strictement interdit d'utiliser le même mot de passe que celui de l'accès réseau communal. Il faut privilégier une adresse courriel de service (p. ex. info@commune.ch) plutôt qu’un accès personnel lors de l’inscription à un site ; le cas échéant, consigner les sites et les identifiants pour ses collègues ou successeurs.

4.7. Téléphonie fixe ou mobile dans le cadre professionnel

4.7.1

Le collaborateur perçoit une indemnité forfaitaire mensuelle pour la mise à disposition de son téléphone et numéro personnel à des fins professionnelles. En contrepartie, son numéro sera communiqué et son appareil servira comme routeur pour ses connexions avec le matériel informatique fourni (p. ex. un VPN).

4.7.2

Les conversations privées, pendant le temps bloqué (présence obligatoire), doivent rester brèves et se limiter au cas de nécessité.

4.7.3

En cas d’absence ou de vacances, le collaborateur prend les mesures nécessaires pour assurer la gestion de ses appels téléphoniques professionnels.

**Art. 5 DÉPART DU COLLABORATEUR**

5.1. Départ

5.1.1

Au départ du collaborateur, et sans disposition expresse contraire, son « adresse de courrier électronique » est immédiatement désactivée.

5.1.2

Le collaborateur prend les dispositions nécessaires à la transmission des informations sur les fichiers qu’il gérait, à ses collègues et/ou successeurs.

5.1.3

Le collaborateur résilie les abonnements faites aux newsletters et qui utilisent son adresse courriel professionnel. Il prend également les mesures utiles pour transmettre les éventuels comptes et identifiants qu'il a dû créer dans le cadre de ses fonctions.et qu'il doit transmettre à son successeur.

**Art. 6 CONTRÔLES ET MESURES DE SÉCURITÉ**

6.1. Contrôles et mesures

6.1.1

Le collaborateur est attaché au respect de la vie privée de ses collègues sur le lieu de travail, et ce en respectant la législation sur la protection des données.

6.1.2

L’exécutif communal se réserve le droit d’accéder à n’importe quel moment à l’ensemble des composants du système, afin d’assurer sa protection et celle des collaborateurs ou afin de déceler des activités illégales.

6.1.3

L’exécutif communal se réserve le droit de procéder à des contrôles anonymes et aléatoires des fichiers. Le traitement des données relevées est confidentiel et soumis à la protection des données.

6.2. Traitement des informations

6.2.1

En cas d’abus constaté, soit lorsque le présent règlement est violé, le président ou le responsable informatique se réserve le droit de faire procéder à des analyses nominatives des fichiers

6.3. Instances compétentes et sanctions en cas d’abus

6.3.1

Après avoir entendu le collaborateur et s’il s’avère que l’utilisation d’internet et des moyens informatiques constitue une violation du présent règlement, l’exécutif communal prend les mesures appropriées pouvant aller jusqu’au licenciement pour justes motifs. Si les agissements du collaborateur sont de nature pénale, l’employeur se réserve tout droit d’agir en justice.

Ainsi adopté par l’exécutif communal du jj.mm.aaaa.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Président Secrétaire communal(e)

**INFORMATIQUE & TÉLÉPHONIE**

Règlement et directives sur l’obligation de confidentialité et sur l’utilisation des outils informatiques, d’internet,
de la messagerie électronique et de la téléphonie fixe ou mobile pour le personnel de commune.

Mme/M. : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

né(e) le : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

confirme avoir reçu, lu et approuvé le règlement susnommé. Il/Elle s’engage à en respecter les règles et en connaît
les conséquences en cas de non-respect de ces dernières.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Lieu, le Signature

**DÉPART DU COLLABORATEUR**

Selon son contrat de travail, le collaborateur s’est engagé à considérer comme secret professionnel, aussi bien avant qu’après son départ, les informations de toutes natures acquises et relatives à son activité professionnelle au sein de
la commune.

Il est interdit de copier et/ou d’emporter tout document (soft, papiers) ou matériel qui a été remis au collaborateur,
dans le cadre de l’exercice de son activité professionnelle, lorsqu’il quitte son poste au sein de la commune.

Le/La soussigné(e) déclare avoir respecté ces prescriptions.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Lieu, le

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Mme/M. Signature