ARASMA
COMITE DE DIRECTION

ASSOCIATION RÉGIONALE
POUR L'ACTION SOCIALE
MORGES-AUBONNE

Tél. 021 / 804 98 98
Fax 021 / 804 98 15
csr@morges.ch

REGLEMENT SUR L'UTILISATION DES OUTILS INFORMATIQUES, D'INTERNET, DE LA MESSAGERIE ELECTRONIQUE ET DU TELEPHONE A LA PLACE DE TRAVAIL

Chapitre I Champ d'application

Art. 1 Objet

Le présent règlement a pour objet la détermination des droits et des devoirs du personnel dans l'utilisation, à sa place de travail, des outils informatiques, d'Internet, de la messagerie électronique et du téléphone.

Il fait partie intégrante du Statut du personnel respectivement du contrat de travail de droit privé.

Le traitement des données est soumis à la législation sur la protection des données.

Chapitre II Principe général

Art. 2 Usage professionnel et privé

Le poste de travail est mis à disposition du collaborateur pour un usage professionnel.

Une utilisation privée est tolérée en dehors des heures de travail, dans la mesure ou elle ne constitue pas un abus, notamment qu'elle ne surcharge pas l'infrastructure informatique (stockage ou transfert de fichier), ne présente pas de caractère illicite, ne vise aucun but lucratif ni ne viole le devoir de fidélité et de diligence de l'employé.

Chapitre III Poste de travail

Art. 3 Responsabilité

Chaque collaborateur possède un espace privé sur le système central afin de lui permettre de stocker des fichiers personnels. L'employeur décline toute responsabilité de la perte des données personnelles.

Art. 4 Modification du poste de travail

La modification du contenu du poste de travail et/ou un usage inapproprié peuvent avoir des effets sur le fonctionnement global du système informatique. La gestion des postes de travail est effectuée par des personnes autorisées sur site ou à distance, en tout temps. Sauf raison professionnelle justifiée, il est notamment interdit de :

a) modifier la configuration matérielle du poste de travail en retirant des composants ou en en installant de nouveaux (par exemple graveur, disque supplémentaire, lecteur DVD, CD-ROM, modem, etc.) ;
b) connecter au poste de travail ou sur le réseau des appareils électroniques sans autorisation (agendas électroniques, téléphones portables, PC portables, clés USB, etc.) ;
c) installer des programmes téléchargés depuis Internet ou reçus par courrier ou en provenance de toute autre source, les modifications effectuées pourront être supprimées sans préavis ;
d) modifier la configuration du poste de travail ou des navigateurs internet ;
e) réaliser des développements informatiques.

Art. 5 Maintenance

Le collaborateur favorisera les opérations découlant des besoins de gestion des postes de travail (activation d'outils d'inventaire et de diagnostic, de télédistribution de logiciels, etc.). Il ne désactivera pas la protection antivirus, ou contournera de quelque moyen que ce soit les dispositifs de sécurité mis en place.

Sur demande d'un utilisateur, le Service informatique peut prendre la main à distance sur les postes de travail afin de résoudre rapidement un problème.

Art. 6 Confidentialité

Lorsqu'il quitte momentanément sa place de travail, le collaborateur veillera à la confidentialité des documents qu'il traite. Pour les postes de travail partagés par plusieurs utilisateurs, le collaborateur veillera à quitter sa session afin de permettre aux autres utilisateurs d'accéder à la machine.

Il traitera son mot de passe de manière confidentielle et ne le divulguera pas à des tiers. Au cas où un mauvais usage en serait fait, sa responsabilité est engagée. Le mot de passe choisi doit être complexe (contenant des chiffres, des majuscules, des minuscules et des caractères spéciaux) et modifié à intervalles réguliers.

Art. 7 Gestion des accès et des fichiers

L'autorisation d'accès aux données informatiques est accordée par le propriétaire de ces données (le service qui gère une application). Il est interdit d'accéder à des données ou à des fichiers pour lesquels l'autorisation n'est pas explicitement donnée, que ces données soient protégées ou non.

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

Toute perte d'un ordinateur ou téléphone portable disposant d'un accès à distance aux données informatiques sera signalé immédiatement au Service informatique, afin que les accès soient désactivés.

Les données confidentielles copiées sur un support mobile (DVD, clé USB, etc.) seront cryptées de manière adéquate. Sur demande, le Service informatique fournira les outils nécessaires.

Chapitre IV Internet

Art. 8 Utilisation d'Internet

L'usage d'Internet est en tout temps est interdit, même en dehors des heures de travail pour :

a) la maintenance de sites personnels de type « blog » ;
b) la visite de sites à caractère érotique, pédophile, pornographique, violent ou raciste ;
c) la visite de sites de jeux ou de paris.

L'utilisation de médias interactifs (type « chat », Facebook ou Youtube par exemple) peut être autorisé uniquement pour des besoins professionnels si nécessaire.

Certains sites sont bloqués par des filtres automatiques.

Le collaborateur s'engage à ne pas copier illégalement des logiciels ou des fichiers protégés par un copyright (musique, film, etc.), à ne pas diffuser des informations appartenant à des tiers sans leur autorisation et à mentionner les sources lors de l'utilisation d'informations en provenance de tiers.

Le collaborateur n'est pas autorisé à s'abonner à des services d'information payants sauf autorisation préalable.

Chapitre V Messagerie électronique

Art. 9 Utilisation de la messagerie électronique

Le règlement d'application de la loi du 24 septembre 2002 sur l'information (RC Info) est applicable par analogie à la messagerie électronique.

Les envois de masse (« spamming ») et de messages « en chaîne » du type « chaînes de chance » (messages à faire suivre à un certain nombre de correspondants) ne sont pas autorisés.

Le collaborateur renoncera à ouvrir des fichiers dont la provenance est douteuse et les détruira. En raison des risques de virus, il est interdit d'ouvrir des fichiers de scripts ou exécutables portant des extensions du type: .exe, .com, .bat, .cmd, .xlm, .vbs, .vb. ou .msi. Cette liste n'étant pas exhaustive.

Le serveur de messagerie est configuré avec un filtre anti-spam pour éviter la réception de « pourriels ».

Afin de garantir la fiabilité et la sécurité de la messagerie, la taille maximale des messages ou de la boîte de messagerie peut être limitée. De même, certains types de pièces jointes peuvent être bloqués.

Art. 10 Distinction entre messages privés et messages professionnels

Les mentions suivantes doivent être utilisées dans l'objet concernant la confidentialité ou le caractère privé/personnel d'un courrier électronique :

a) Confidentiel : un courrier électronique dont l'objet contient ce mot ne peut être ouvert que par les personnes ayant un accès explicite, en lecture, à la boîte aux lettres. Le traitement de l'information doit être fait de la même manière qu'un courrier confidentiel papier.

b) Privé ou Personnel : un courrier électronique dont l'objet contient ce mot ne peut être ouvert que par la personne à qui ce courrier électronique est destiné. Il ne doit contenir aucune information professionnelle.

L'employeur n'a le droit ni de consulter ni de traiter d'une quelconque manière les messages privés signalés comme tels. Les expéditeurs internes ou externes de messages privés doivent être informés du fait que les messages privés non signalés comme tels sont susceptibles d'être lus par une tierce personne.

Lorsque rien n'indique la nature du message et que les éléments d'adressage ne permettent pas non plus de déterminer qu'il s'agit d'un message privé, l'employeur part de l'idée qu'il s'agit d'un message professionnel.

En cas de panne, le Service informatique pourra accéder, avec l'accord de l'utilisateur, à la boîte de messagerie complète s'il n'y a pas d'autre solution pour rétablir le bon fonctionnement.

Art. 11 Gestion du courrier électronique d'un collaborateur absent

Pendant ses absences, le collaborateur prendra les mesures nécessaires pour assurer un suivi de ses courriers électroniques professionnels en activant son agent d'absence ou en déléguant l'accès à sa messagerie. En cas d'oubli ou d'absence prolongée non prévisible, le Service informatique se réserve le droit d'accéder à la messagerie du collaborateur et de prendre les mesures nécessaires pour assurer un suivi des courriers électroniques professionnels.

Chapitre VI Téléphonie

Art. 12 Utilisation de la téléphonie

Les conversations privées demeureront exceptionnelles et brèves. Ces règles sont également valables pour les appels entrants.

Les collaborateurs doivent privilégier les appels depuis et vers les postes fixes avant de composer le numéro du mobile.

Chapitre VII Départ du collaborateur

Art. 13 Directives de départ

Le collaborateur avant la cessation de ses rapports de services transférera à qui de droit les affaires pendantes y compris les messages électroniques. Il effacera ses données personnelles de sa boîte de messagerie électronique et de son espace personnel.

Son compte de courrier électronique et ses comptes informatiques seront bloqués au plus tard le dernier jour de travail. Sa boîte aux lettres et autres supports de données personnels seront effacés.

Les personnes qui enverront un message à l'adresse bloquée ne seront pas automatiquement informées du fait qu'elle n'existe plus.

Chapitre VIII Sanctions

Art. 14 Sauvegarde de l'historique des communications

La plupart des activités effectuées à l'aide de moyens informatiques sont consignées dans des fichiers, appelés « fichiers journaux ». Le Service informatique garde un historique des communications établies. Il indique pour chaque utilisateur ou poste de travail l'adresse des sites internet consultés et l'expéditeur/destinataire ainsi que l'objet des messages envoyés (mais pas le contenu des messages).

Lors de dysfonctionnements, le Service informatique peut analyser les fichiers journaux pour en déterminer la cause.

Art. 15 Contrôle

Art. 15.1 Contrôle global

La Direction peut ordonner au Service informatique des analyses anonymes des fichiers journaux. L'analyse est effectuée de manière telle qu'elle ne permette pas l'identification de l'utilisateur.

Pour ce faire, le Service informatique peut extraire les statistiques suivantes :

a) une statistique globale des sites internet les plus utilisés ;
b) une statistique du volume de données moyen échangé par poste de travail ;
c) une statistique du nombre de messages moyen envoyé et reçu par utilisateur ;
d) le montant des factures de téléphonie.

Art. 15.2 Contrôle personnalisé

Un contrôle personnalisé sera ordonné par la Direction en cas d'abus et dans le cadre d'une procédure disciplinaire ou d'une enquête administrative elle peut prendre les formes suivantes :

a) liste détaillée des sites internet visités par un utilisateur ;
b) liste détaillée du nombre de messages électroniques envoyés et reçus incluant les éléments d'adressage, l'objet, la date et l'heure, le type et le volume des fichiers attachés. Il ne porte pas sur le contenu des messages ;
c) consultation des factures détaillées de téléphones.

Art. 16 Sanctions

En cas d'infraction au présent règlement, la Direction peut prononcer des sanctions disciplinaires ou des avertissements tels que prévus par le Statut du personnel, contre les collaborateurs fautifs.

Pour les cas graves la résiliation de contrat pour justes motifs peut être prononcé.

Le blocage de l'accès à Internet peut également être prononcé.

Art. 17 Entrée en vigueur

Le présent règlement entre en vigueur le 1er mars 2011 et abroge le document intitulé Gestion d'accès et utilisation des PC du 17 janvier 2000.

Ainsi adopté par le Comité de direction dans sa séance du 15 février 2011.

au nom du comité de direction ARASMA

La présidente	Le directeur
Gisèle Burnet	Daniel Vouillamoz