Charte informatique du Campus La Mouillère
Personnel

1.Définitions

"Equipements informatiques" : désigne l'ensemble physiques des matériels, équipements, outils informatiques mis à disposition par le Campus de La Mouillère aux utilisateurs.

"Utilisateur" : désigne toute personne qui utilise les systèmes d'information du Campus et les équipements informatiques quel que soit son statut, et notamment les salariés, les intérimaires, les stagiaires, ou toute personne qui a obtenu un droit d'utilisation du système d'information du Campus de La Mouillère ou de ses équipements informatiques.

"Système d'information" (SI) : ensemble de ressources du Campus qui permettent la gestion de l'information.

2.Les Accès

L'accès à certains éléments du système d'information (comme la messagerie électronique ou téléphonique, les sessions sur les postes de travail, le réseau, certaines applications ou services interactifs) est protégé par des paramètres de connexion (identifiant, mot de passe).
Chaque utilisateur reçoit un droit d'accès individuel qui se matérialise par tout moyen logique (code utilisateur, mot de passe...)

Ces paramètres sont personnels à l'utilisateur et doivent être gardés confidentiels. Ils permettent en particulier de contrôler l'accès des utilisateurs. Ils ne doivent être communiqués à personne, ni responsable hiérarchique, ni informatique.
Dans la mesure du possible, ces paramètres doivent être mémorisés par l'utilisateur et ne pas être conservés, sous quelque forme que ce soit. En tout état de cause, ils ne doivent pas être transmis à des tiers ou aisément accessibles.

Lorsqu'ils sont choisis par l'utilisateur, les paramètres doivent respecter un certain degré de complexité et être modifiés régulièrement.

Ce droit d'accès cesse automatiquement lors d'un départ ou s'il est constaté que l'utilisateur a enfreint l'une des obligations imposées par la présente charte.

2.1 Accès la messagerie

Chaque salarié dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique Gmail.

L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée qu'un courrier manuscrit et peut rapidement être communiqué à des tiers.

Il convient de prendre garde au respect d'un certain nombre de principes, afin d'éviter les dysfonctionnements du système d'information, de limiter l'envoi de messages non sollicités.
L'utilisateur ne doit pas ouvrir, ni répondre à des messages électroniques tels que spam, messages électroniques répétés, ni les transférer.
Il s'engage, dans pareil cas, à les détruire immédiatement et à avertir le responsable des systèmes d'information en cas d'abus manifeste de fréquence ou de volume.

L'utilisateur est informé et accepte qu'en cas d'absence prolongée et pour la continuité des services, la direction des systèmes d'information se réserve le droit d'accéder à sa messagerie et à ses dossiers professionnels, et ce sans son consentement préalable.

En cas d'absence, l'utilisateur devra activer la notification d'absence afin de prévenir toute discontinuité dans le traitement des messages et permettre à ses interlocuteurs de prendre des mesures appropriées.

Pour appliquer le principe du droit à la déconnexion, les mails doivent être envoyés prioritairement aux heures d'ouverture de l'établissement de 8 heures à 18 heures, du lundi au vendredi.

2.2 Accès internet

Au sein de l'établissement, les utilisateurs ont accès à internet via le réseau sécurisé de La Mouillère.
Le code wifi "Mouillère" est réservé uniquement au personnel et ne doit être transmis ni aux apprenants ni aux personnes extérieures à l'organisation.
Pour des raisons de sécurité ou de déontologie, l'accès à certains sites peut être limité ou prohibé par la direction informatique qui est habilitée à imposer des configurations du navigateur et à installer des mécanismes de filtrage limitant l'accès à certains sites (proxy).

La connexion à des sites Internet dont le contenu est contraire à l'ordre public, aux bonnes mœurs ou à l'image de marque du Campus La Mouillère, ainsi qu'à ceux pouvant comporter un risque pour la sécurité du système d'information est interdite.

2.3 Accès à la téléphonie

Pour leur activité professionnelle, certains utilisateurs peuvent disposer d'un téléphone fixe et/ou mobile.

Concernant l'utilisation des terminaux mobiles (smartphone) connectés à internet, les règles édictées dans la présente charte s'appliquent identiquement.

De plus, il est rappelé que l'envoi de SMS est réservé aux communications professionnelles et qu'il engage la responsabilité de l'émetteur au même titre que l'envoi d'un courriel.

L'utilisateur est informé qu'un journal des communications, entrantes et/ou sortantes, est accessible par la direction s'agissant tant de la téléphonie fixe que mobile. Les utilisateurs sont informés que les relevés de communication peuvent faire l'objet d'un contrôle.

Engagements de l'utilisateur :

L'utilisateur s'engage en outre à :

- prévenir sans délai en cas de perte, vol ou faille de sécurité ;
- mettre en œuvre tous les moyens de sécurité prévus par les fonctionnalités du smartphone (code d'accès, verrouillage clavier, code pin...)
- se déconnecter de toutes applications après usage et ne pas rester connectés par défaut ;
- être vigilants vis à vis des données contenues dans le smartphone

Utilisation personnelle du téléphone

L'utilisation à caractère personnel du téléphone, fixe ou mobile, est tolérée, à condition qu'elle reste dans des limites raisonnables en termes tant de temps passé que de quantité d'appels.

Les surcoûts pour l'entreprise engendrés par l'utilisation de la téléphonie à des fins personnelles devront être remboursés par les utilisateurs concernés. Il s'agit tout particulièrement des appels à des numéros surtaxés et des appels depuis l'étranger ou à destination de l'étranger, au sens de la facturation téléphonique.

2.4 Accès à l'extérieur du Campus de La Mouillère (télétravail, déplacement professionnel...)

Il convient de préciser que l'ensemble des dispositions de la présente charte sont applicables aux utilisateurs accédant au système d'information et de communication du Campus de La Mouillère à distance. Dans le cadre de ses déplacements professionnels, peu importe leur durée ou leur fréquence, l'utilisateur se doit d'adopter une attitude de prudence et de réserve au regard des informations et des ressources du système d'information qu' il pourrait être amené à accéder, manipuler ou échanger.

En particulier, il est déconseillé d'utiliser les systèmes de connexion wifi dans les lieux publics.

2.5 Accès au matériel informatique

Dans les salles de cours

Du matériel informatique (ordinateur, VPI...) se trouve dans chaque salle de cours.
L'utilisateur doit se connecter à sa session et se déconnecter à la fin de sa séance.
Les câbles ne doivent pas être débranchés et le formateur ne doit pas quitter la salle de cours sans avoir vérifié l'état de matériel informatique (câble branché, souris et clavier rangés...)
Il en est de même pour Les salles informatiques (CAO/DAO, Learning center 1): le formateur doit veiller au bon état du matériel (ordinateur, télévision...) et vérifier que les feuilles de suivis sont remplies pour tous les postes de travail.
Le formateur se doit d'informer dans les plus brefs délais tout problème informatique par mail à maintenance-si@lamouillere.fr

Dans les bureaux

Des ordinateurs sont à disposition des personnels administratifs dans chaque bureau.
L'utilisateur doit se connecter à sa session et se déconnecter dès qu'il quitte son bureau.
Il doit veiller au bon état du matériel et signaler tout problème au service SI (maintenance-si@lamouillere.fr ou par téléphone poste 130).

2.5 Fin d'accès au système d'information (départ)

Lors de son départ du Campus de La Mouillère, l'utilisateur doit respecter la procédure de départ et remettre l'ensemble des moyens informatiques et de communication électronique qui lui ont été remis (ordinateur, périphériques, mobile, carte d'accès, moyen d'authentification à distance, badges, supports de stockage, etc.) en bon état général de fonctionnement et ne conserver aucun matériel ou aucune donnée permettant d'accéder au système d'information.
De plus, l'utilisateur s'interdit, avant son départ, de détruire des informations et des données professionnelles.

Sauf nécessité liée à la continuité du service et pour un temps raisonnable qui ne saurait excéder trois mois, le compte messagerie de l'utilisateur est supprimé le jour de son départ et de ce fait son accès à google workspace.

Dans le cas où le compte messagerie est toujours actif, même après le départ d'un utilisateur, une redirection des messages peut être mise en place par le Campus de La Mouillère vers l'utilisateur ayant repris le poste ou toute autre personne occupant une fonction similaire.

Ses identifiants sont également désactivés.

3.Rappel des principales lois

La Loi n° 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, dite Loi Informatique et Libertés, l'ordonnance n°2018-1125 du 12 décembre 2018, ainsi que le Règlement général sur la protection des données (RGPD) viennent définir les conditions dans lesquelles des traitements de données à caractère personnel peuvent être opérés.

La Loi Informatique et Libertés et le RGPD instituent au profit des Personnes concernées par les traitements réalisés par les utilisateurs des droits que la présente charte vient protéger et respecter, tant à l'égard des utilisateurs que des tiers.
A cet égard, le responsable des traitements s'engage vis à vis des utilisateurs à :

- ne pas utiliser les données à caractère personnel auxquelles ils peuvent accéder à des fins autres que celles prévues par leurs attributions ;
- ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
- ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de leurs fonctions ;
- prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de leurs attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;
- d'assurer, dans la limite de leurs attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
- ne pas accéder, tenter d'accéder ou supprimer les données en dehors de leurs attributions ;
- respecter les droits des personnes concernées (droit d'accès, de rectification, d'opposition, effacement...) conformément aux procédures mises en place.
- en cas de cessation de leurs fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

Aussi, le responsable des traitements s'engage, et par voie de conséquence les utilisateurs, par le respect de la présente charte, à respecter les principes fondamentaux de la protection des données à caractère personnel, à savoir notamment la minimisation de la collecte et la préservation de la confidentialité, de l'intégrité et de la sécurité des données à caractère personnel.

Les utilisateurs sont au cœur de la protection des données à caractère personnel, et par conséquent des libertés et de la vie privée des personnes concernées.

Contrôle du système d'information:

L'utilisateur est informé que le responsable des systèmes d'information (qui doit veiller au fonctionnement normal et à l a sécurité des réseaux et systèmes informatiques) est conduit de par ses fonctions, à avoir accès à l'ensemble des informations relatives aux utilisateurs (messages, connexion à Internet, analyse de google workspace), mais demeure soumis aux règles encadrant le secret professionnel le responsable des systèmes d'information dûment mandatée par le directeur peut contrôler les systèmes d'information, afin de vérifier que ce dernier respecte les clauses définies dans la présente charte.
En cas de suspicion de manquement grave aux dispositions de la présente charte, la Direction pourra procéder à toutes les mesures d'investigation utiles, dans le respect des règles en vigueur.

Tout logiciel installé illicitement ou tout fichier suspect sera supprimé par le responsable des systèmes d'information dès le constat de leur présence sur le poste de travail.

Le caractère « non professionnel » des répertoires informatiques clairement identifiés comme « privé » ou « personnel », ne fait pas obstacle à des modalités de contrôle dans les conditions précitées.

4. Attestation de lecture et d'acceptation de la charte informatique

Important par la signature de ce document vous confirmez avoir pris connaissance de la charte informatique et vous vous engagez à la respecter.

Je soussigné (e)
Nom :
Prénom :
Certifie avoir lu et accepté la charte informatique du Campus de La Mouillère du bon usage des ressources informatiques.

A _____ le _____ Signature de l'utilisateur