CHARTE INFORMATIQUE DU CAMPUS DES SICAUDIERES

1/ PRÉAMBULE

Le Campus des Sicaudières met en œuvre un système d'information et de communication nécessaire à son activité, comprenant notamment un réseau informatique et téléphonique, ainsi que des outils mobiles.

Les personnels, élèves et étudiants, dans l'exercice de leurs fonctions, sont conduits à utiliser les outils informatiques et/ou téléphoniques mis à leur disposition et à accéder aux services de communication de l'établissement.

L'utilisation du système d'information et de communication doit se faire exclusivement à des fins professionnelles et pédagogiques.

Dans un but de transparence à l'égard des utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée du système d'information et de communication, la présente charte pose les règles relatives à l'utilisation de ces ressources. Elle définit aussi les moyens de contrôle et de surveillance de cette utilisation mise en place, non seulement pour la bonne exécution du travail de chacun, mais aussi dans le cadre de la responsabilité pénale et civile de l'employeur. Elle ne remplace en aucun cas les lois en vigueur que chacun est censé connaître.

2/ CHAMP D'APPLICATION

2.1 Utilisateurs concernés

La présente charte s'applique à l'ensemble des utilisateurs du système d'information et de communication du Campus des Sicaudières, quel que soit leur statut, y compris les stagiaires, employés de sociétés prestataires, visiteurs occasionnels. Elle sera annexée aux contrats de prestations.

2.2 Système d'information et de communication

Le système d'information et de communication du Campus des Sicaudières est notamment constitué des éléments suivants : ordinateurs (fixes ou portables), tablettes numériques, périphériques y compris clés USB, réseau informatique (serveurs, routeurs et connectique), photocopieurs, téléphones, logiciels, fichiers, données et bases de données, système de messagerie, connexion internet, extranet, abonnements à des services interactifs...

Pour des raisons de sécurité du réseau, est également considéré comme faisant partie du système d'information et de communication le matériel personnel des salariés et apprenants connecté au réseau de l'établissement, ou contenant des informations à caractère professionnel concernant l'établissement.

2.3 Autres accords sur l'utilisation du système d'information

La présente charte ne préjuge pas des accords particuliers pouvant porter sur l'utilisation du système d'information et de communication par les institutions représentatives, l'organisation d'élections par voie électronique, la mise en télétravail ou le suivi pédagogique à distance.

3/ CONFIDENTIALITÉ

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 dispose d'un «compte personnel» sur le réseau lui donnant des droits particuliers et un répertoire personnel pour la sauvegarde de son travail. Chacun doit travailler en se connectant au réseau sous son nom et en utilisant son mot de passe qui doit absolument rester confidentiel. **Chacun est responsable de ce qui se trouve dans son répertoire et de ce qui se fera sous son nom de connexion. Le répertoire personnel ne sert qu'à conserver des travaux personnels ou des fichiers utiles pour son travail**. Aucun programme exécutable (du type *.exe ou *.com) ou économiseur d'écran ne doit être copié dans le répertoire personnel ou installé sur un poste de travail sans raison pédagogique valable. Il est interdit d'amener ou de télécharger des programmes, de copier ou de modifier ceux qui sont installés sur les ordinateurs ou le réseau.

4/ SÉCURITÉ

4.1 Rôle de l'établissement

- CONTRÔLES TECHNIQUES : L'établissement dispose de moyens techniques pour procéder à des contrôles de l'utilisation du service sur toute partie qui en dépend : consultation de la mémoire cache, disques durs, contrôle des flux, installation de limites d'accès au serveur, utilisation d'un pare-feu. L'établissement garantit l'utilisateur que seuls ces moyens de contrôle peuvent être mis en œuvre dans un strict respect de la confidentialité et de la vie privée.
- MISSIONS DES ADMINISTRATEURS : Chaque ordinateur et chaque réseau est géré par un ou plusieurs administrateurs. Ce sont eux qui gèrent les comptes des utilisateurs. De manière générale, les administrateurs ont le droit de faire tout ce qui est nécessaire pour assurer le bon fonctionnement des moyens informatiques du lycée. Ils informent, dans la mesure du possible, les utilisateurs de toute intervention susceptible de perturber ou d'interrompre l'utilisation habituelle des moyens informatiques. En cas d'urgence, les administrateurs informatiques pourront être amenés à prendre toutes dispositions propres à assurer l'intégrité et la sécurité des systèmes et des utilisateurs. Les administrateurs ont la possibilité de consulter les informations stockées par les utilisateurs (sauf le contenu des messages électroniques). Ils se réservent le droit de supprimer les informations privées n'ayant pas lieu d'être stockées sur le réseau du lycée (jeux, logiciels divers, fichiers musicaux, images, vidéos…) sans en avertir le propriétaire. Les administrateurs peuvent être amenés à surveiller les sessions des utilisateurs. Cette surveillance exceptionnelle est effectuée en cas d'agissements suspects et en liaison avec le chef d'établissement.
- PRÉSERVATION DE L'INTÉGRITÉ DU SERVICE : L'utilisateur est responsable de l'usage qu'il fait du service. Il assure, à son niveau, la sécurité du service et s'engage à ne pas perturber volontairement son fonctionnement.
- DISPONIBILITÉ ET FIABILITÉ DU SERVICE : L'établissement s'efforce de maintenir le service accessible de manière permanente, mais n'est tenu à aucune obligation d'y parvenir. L'établissement peut en interrompre l'accès, pour des raisons techniques ou pour toute autre raison, sans qu'il puisse être tenu pour responsable des conséquences de ces interruptions aussi bien pour l'utilisateur que pour tous tiers. L'établissement ne garantit pas que le service soit exempt de toute interruption, retard, incident de sécurité ou erreur.

4.2 Responsabilité de l'utilisateur

L'informatique au lycée est un outil de travail, le matériel informatique doit être manipulé avec précaution dans un environnement propre, c'est pourquoi l'introduction de boissons et nourriture est proscrite dans les lieux de formation équipés de matériel informatique.

Ne pas débrancher un périphérique, déplacer un ordinateur ou une imprimante sans autorisation préalable, enfin, « fermer » correctement les logiciels utilisés et éteindre le poste de travail après chaque utilisation.

L'utilisateur s'engage à une utilisation rationnelle et loyale du service et notamment du réseau, des ressources informatiques, afin d'en éviter la saturation ou le détournement à des fins personnelles.

L'utilisation d'outils informatiques connectés au réseau WIFI du lycée est autorisée en faisant la demande aux administrateurs du réseau.

Des contrôles identiques aux postes fixes pourront être effectués par les administrateurs informatiques. Tout utilisateur, qui ne suivra pas ces règles, verra son autorisation retirée. Il pourra être par ailleurs sanctionné s'il ne respecte pas la charte y compris à partir de son matériel personnel. Ces règles de «bon usage» sont susceptibles d'évoluer sous le contrôle de la direction, notamment en fonction de l'état de la technique et des pratiques constatées sur le réseau.

Il est recommandé de renommer tous vos supports amovibles (clés USB, disques durs amovibles) par votre nom d'utilisateur de session afin de faciliter la restitution de ces supports en cas d'oubli ou de perte.

La RGPD (Réglementation Générale de Protection des Données) vous rend responsable (en cas de perte ou de vol) des données personnelles que vous stockez sur vos supports amovibles, c'est pourquoi il est indispensable de crypter vos lecteurs de données amovibles (BitLocker est disponible sur tous les ordinateurs de l'établissement).

Dans le même esprit, toute session ouverte à votre nom vous expose à une fuite voire un vol de données personnelles relevant de la RGPD, d'où l'importance de fermer votre session à la fin de chaque utilisation, ou de la verrouiller entre deux usages.

5/ INTERNET

FILTRAGE DES SITES INTERNET : Un accès à Internet est attribué aux utilisateurs afin de permettre la consultation des sites au nom de l'établissement. Ce dernier met en œuvre des systèmes de filtrage afin d'interdire l'accès à certains sites Internet dont le contenu lui semble illicite, en contradiction ou sans rapport avec ses objectifs éducatifs, ou requiert l'âge de la majorité.

CONTROLE DES PAGES WEB : L'établissement se réserve le droit de contrôler le contenu hébergé sur tout serveur mis en œuvre dans le cadre de l'activité en vue de s'assurer du respect des conditions d'utilisation du service énoncées par la présente charte. L'établissement se réserve le droit de suspendre l'accès au service d'hébergement des contenus en cas de non respect de la Charte et notamment dans l'hypothèse où l'utilisateur aurait diffusé sur ses pages Web un contenu manifestement illicite.

6/SANCTIONS

Tout contrevenant au respect de cette charte s'expose à des sanctions à l'initiative de l'employeur pour les salariés, et du conseil de discipline pour les apprenants. Les détériorations volontaires de matériels informatiques pourront être facturées.

Il est rappelé que toute personne sur le sol français doit respecter l'ensemble de la législation applicable, notamment dans le domaine de la sécurité informatique :

• la loi du 6/1/78 dite `` informatique et liberté '' ;

• la législation relative à la fraude informatique (article 323-1 à 323-7 du Code pénal);

• la loi du 10/07/91 relative au secret des correspondances émises par voie de télécommunication ;

• la législation relative à la propriété intellectuelle ;

• la loi du 04/08/1994 relative à l'emploi de la langue française ;

• la législation applicable en matière de cryptologie, notamment l'article 28 de la loi du 29/12/90 sur la réglementation des télécommunications dans sa rédaction issue de l'article 17 de la loi du 26/07/96 et par ses décrets d'application du 24/02/98, 23/03/98 et 17/03/99;

• les législations sur l'audiovisuel et les télécommunications en ce qui concerne les grands principes applicables aux communications publiques et privées.

• la loi n° 2018-493 du 20 juin 2018 afin de mettre en conformité le droit français avec le cadre juridique européen. Elle permet la mise en œuvre concrète du RGPD et de la Directive « police-justice », applicable aux fichiers de d'ordre pénal.

Je soussigné,

Nom :

Prénom :

Qualité ou Classe :

Utilisateur des moyens informatiques et réseaux de l'établissement " Les Sicaudières", reconnaît avoir été doté d'un compte utilisateur sur un des serveurs de l'établissement,

Déclare avoir pris connaissance de la présente charte de bon usage de l'informatique et des réseaux et m'engage à la respecter.

Lu et approuvé

Signature

Fait à Bressuire en 2 exemplaires le mardi 3 mai 2022