GROUPE
Saint-Bénigne

CHARTE INFORMATIQUE

SUR LE BON USAGE DES OUTILS INFORMATIQUES ET DE COMMUNICATION MIS À DISPOSITION PAR LE GROUPE SAINT BENIGNE

L'établissement Lycée Saint Bénigne, appelé Groupe ci-après, met en œuvre *un système d'information* nécessaire à son bon fonctionnement ainsi qu'à l'exercice de ses missions. Dans ce contexte, le service informatique du Groupe met à la disposition des *utilisateurs* des *outils informatiques et de communication* à des fins scolaires, pédagogiques ou professionnelles.

La présente Charte définit les règles d'accès et d'utilisation de ces outils, énonce des droits et devoirs à l'attention des utilisateurs et informe des moyens de contrôle organisés dans un souci de loyauté et de transparence. La présente Charte a été annexée au Règlement intérieur. Les évolutions du système d'information susceptibles d'affecter le contenu de la présente Charte pourront faire l'objet de modifications de la Charte.

Le service informatique peut répondre à toute question relative aux règles définies dans la présente Charte. La personne en charge de la protection des données au sein du Groupe se tient à la disposition par email (dpo@groupe-sb.org) pour les dispositions de la Charte relevant du droit de la protection des données ou pour exercer le droit d'alerte (loi 2016-1691 du 9 décembre 2016). Tout signalement abusif ou déloyal peut être puni de 2 ans d'emprisonnement et 30 000 euros d'amende.

Les règles de la présente Charte s'appuient sur les textes suivants :

- le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après « RGPD ») ;
- la loi n°78/17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés (ci-après : la « loi Informatique et Libertés »), et les textes nationaux applicables à la protection des données personnelles ;
- les articles 9 et 1194 du Code civil ;
- les articles 226-16 à 226-24, et 323-1 à 323-7 du Code pénal ;
- l'article L.335-2 du Code de la propriété intellectuelle.

1) REGLES APPLICABLES AU SYSTEME D'INFORMATION

Le Groupe entend prendre toutes les précautions utiles pour préserver la sécurité des données placées sous sa responsabilité et empêcher qu'elles soient déformées, endommagées, ou accédées par des tiers non autorisés, ainsi que pour garantir le bon fonctionnement de son système d'information.

GROUPE
Saint-Bénigne

A. Le système d'information est mis à disposition pour un usage pédagogique

L'utilisation du système d'information est limitée à un usage scolaire. L'utilisation à titre privé de ce système est toutefois tolérée, sous réserve d'être raisonnable et de ne perturber, ni le travail de l'utilisateur, ni celui des autres utilisateurs, ni la sécurité du système.

Un utilisateur peut conserver des données personnelles sur son poste de travail dans un fichier nommé « privé » ou « personnel » en veillant à ce que le fichier respecte une taille raisonnable. Les autres éléments sont présumés avoir un caractère pédagogique, autorisant, de fait, le service informatique à prendre connaissance :

- des fichiers et dossiers stockés ou transmis à l'aide de l'outil informatique mis à sa disposition par le Groupe ;
- des supports amovibles, mêmes personnels, connectés à un outil informatique mis à disposition d'un utilisateur par le Groupe pour les besoins de son travail ;
- des messages électroniques adressés ou reçus par un utilisateur sur la messagerie électronique du Groupe.

B. Consignes d'utilisation du système d'information

La mise à disposition de tout outil informatique ou de communication est assortie de consignes d'utilisation ou de sécurité (communiquées par le personnel habilité ou par service informatique) que les utilisateurs doivent respecter.

Les utilisateurs doivent veiller à ne pas dégrader ou changer la configuration des outils mis à disposition et considérer que toute modification d'un outil informatique ou de communication ne peut être réalisée que par le service informatique, ou avec son accord exprès.

1. Compte utilisateur

Un contrôle d'accès permet d'identifier toute personne utilisant un poste ou un terminal de connexion. Cette identification unique permet l'attribution de droits propres à chaque utilisateur sur le système d'information. Ces droits d'accès sont soumis à l'autorisation préalable du service informatique et peuvent être révoqués.

L'utilisateur est personnellement responsable de l'utilisation qui peut en être faite et ne doit en aucun cas communiquer son mot de passe à un tiers, quel qu'il soit. Tout usage d'un identifiant et d'un mot de passe appartenant à un autre utilisateur est constitutif d'une usurpation d'identité passible de sanction. Il est déconseillé de conserver son mot de passe sur papier ou sur tout autre support non sécurisé.

Lorsque l'utilisateur s'absente de son poste de travail, il doit fermer les documents et la session en cours. Il ne doit pas quitter son poste de travail sans, au minimum, verrouiller sa session.

GROUPE
Saint-Bénigne

2. Utilisation, enregistrement et sauvegarde des données

Toutes les informations contenues dans le système d'information doivent être traitées de manière à assurer leur confidentialité et à garantir leur sécurité. Elles ne doivent être communiquées qu'aux personnes qui sont habilitées à en prendre connaissance.

L'utilisateur, destinataire de données **par erreur** doit les supprimer et avertir le DPO.

3. Perte d'un outil informatique

La perte, le vol ou le bris d'un outil informatique mis à disposition par le Groupe doit être sans délai porté à la connaissance du service qui l'a mis à disposition conformément à la convention de mise à disposition, le cas échéant. L'utilisateur précisera quel paramétrage de sécurité avait été mis en œuvre ainsi que la nature des données qui y étaient stockées.

4. Modalités de contrôle

Le service informatique doit veiller à la protection, à la sécurité, à la maintenance, au bon fonctionnement et à la qualité de services des ressources du système d'information dont il a la charge. Notamment : la sauvegarde des données, l'intégrité des données, la preuve des dates de création ou de diffusion, l'absence d'intrusion, le défaut de licence.

Le service informatique peut contrôler et surveiller toutes les activités effectuées sur le système d'information et de communication, répondant strictement à la finalité de la protection du système d'information, dans le respect des textes juridiques applicables et de la déontologie professionnelle. Les données traitées à l'occasion du contrôle ne sont pas conservées, sauf en cas de sanction ou à la demande des autorités judiciaires. L'utilisateur doit restituer ou confier tout périphérique, à la demande du service informatique, lorsqu'il est avéré que ce périphérique compromet la sécurité du système d'information.

L'utilisateur est informé que le service informatique peut avoir accès à l'ensemble des composants du système d'information et que ses activités sont enregistrées dans des journaux, conformément à l'article 6 de la loi 2006-64.

5. Interdictions et obligations générales

Il est interdit d'utiliser le système d'information pour commettre un acte susceptible d'engager la responsabilité de son auteur ou celle du Groupe.

Tout utilisateur est tenu de respecter la législation en vigueur, pour rappel :

- au respect des droits des personnes (respect de la vie privée, du secret des correspondances, du droit à l'image) ou à la sensibilité d'un autre utilisateur notamment par des messages ou images provocants, malveillants, menaçants, injurieux ou diffamatoires ;

GROUPE
Saint-Bénigne

- à la malveillance informatique : l'utilisateur doit veiller à éviter toute altération, suppression ou modification des éléments du système ou toute entrave à son bon fonctionnement ;
- à l'ordre public et aux bonnes mœurs ;
- à la propriété intellectuelle : respect des droits de propriété (licence d'utilisation de logiciels, la reproduction ou l'utilisation de données protégées par le droit d'auteur ou de droit voisin) ;
- aux traitements de données à caractère personnel.

RAPPEL DES REGLES ELEMENTAIRES DE SECURITE

Des pirates informatiques peuvent s'appuyer sur l'imprudence des utilisateurs à leur insu.

- ✓ Ne communiquez jamais vos mots de passe, à qui que ce soit.
- ✓ Verrouillez votre session en quittant votre poste de travail et éteignez-le en partant.
- ✓ Signalez toute tentative de fraude, usurpation d'identité.
- ✓ Ne cliquez jamais en cas de doute, sur un lien ou une pièce jointe dans un message.
- ✓ Ne vous contentez pas des informations affichées pour légitimer l'expéditeur.
- ✓ Ne laissez jamais qui que ce soit prendre le contrôle à distance (sauf service info).

2) REGLES APPLICABLES AUX MATERIELS ET LOGICIELS

A. Utilisation des matériels et logiciels

L'utilisateur est tenu de les manipuler de façon à éviter tout risque de détérioration ou de casse. Il est interdit de boire ou de manger à proximité des matériels informatiques mis à disposition. Les personnes disposant d'un périphérique du Groupe doivent également respecter cette règle, quel que soit le lieu d'utilisation.

Il est interdit de déplacer, débrancher, reconfigurer le matériel informatique fixe. Tout bris ou mauvais fonctionnement de matériel appartenant au Groupe doit être immédiatement signalé au service informatique.

L'utilisateur est prié d'éteindre, par arrêt complet, l'ensemble de son matériel informatique en quittant son poste à l'issue de sa journée de cours.

B. Utilisation des logiciels

Les logiciels installés sur les postes de travail ont fait l'objet de l'acquisition par le Groupe des droits et licences d'utilisation et ne peuvent être utilisés que dans ce cadre. La duplication d'un logiciel sans contrat de licence est assimilée à de la contrefaçon.

GROUPE
Saint-Bénigne

C. Introduction de matériels et logiciels externes

L'utilisateur peut connecter son périphérique personnel au réseau wifi de l'établissement tant qu'il est conforme aux standards de sécurité :

- système d'exploitation à jour des correctifs de sécurité ;
- antivirus et signatures à jour ;
- absence de logiciel malveillant ;
- présence de licence des logiciels installés.

Sont interdits, sauf autorisation du service informatique :

- le branchement d'un équipement externe à un poste ou au réseau filaire ;
- l'installation d'un logiciel sur un poste du Groupe ;
- l'utilisation d'un logiciel de jeu ou de téléchargement connecté au réseau.

Le service informatique se réserve le droit de supprimer tout logiciel non autorisé. Ces règles peuvent évoluer vers une interdiction partielle ou totale de la connexion au wifi.

3) REGLES APPLICABLES AUX OUTILS DE COMMUNICATION

A. Messagerie, messagerie instantanée et partage de fichiers

Le Groupe met à disposition des utilisateurs (durant la période de présence au sein du Groupe), via la plateforme Microsoft Office 365, un espace de travail collaboratif incluant notamment une messagerie, une messagerie instantanée et un partage de fichiers, nommés « outils de communication ». Le Groupe garde l'entière propriété des comptes et licences, et a donc la possibilité de gérer sans contrainte l'ensemble de ses éléments.

1. Consignes d'utilisation

L'utilisateur est responsable de la bonne utilisation des outils de communication, et des contenus qu'il adresse.

BON USAGE DE LA MESSAGERIE

- ✓ Renseignez l'objet : un titre concis détermine l'intérêt de votre destinataire à vous lire.
- ✓ Soignez la présentation du message : mettez en forme un minimum pour faciliter la lecture.
- ✓ Faites un usage modéré des majuscules, des caractères gras, des points d'exclamation.
- ✓ Soyez prudent si vous faites de l'humour : la messagerie n'est pas le bon vecteur.
- ✓ Tenez compte des différences culturelles : attention aux problèmes de compréhension.
- ✓ Visez la cible : envoyez sans envahir, choisissez qui mettre en copie et ne répondez pas 'à tous'.
- ✓ Ne répondez pas systématiquement 'à chaud'. Vous ne le diriez pas ?... Alors ne l'écrivez pas !
- ✓ Si le message vous parvient en dehors des heures de travail ou des jours ouvrés, merci de considérer qu'il n'appelle pas de réponse avant le retour de ces conditions

La messagerie ne doit pas être utilisée à des fins publicitaires. Les messages de promotion des activités pédagogiques et associatives doivent être validés par un enseignant référent.

GROUPE
Saint-Bénigne

Les messages collectifs utilisant des groupes de destinataires sont réservés aux diffusions internes, et doivent être utilisés avec discernement.
L'utilisateur est invité à limiter l'impression papier de ses messages, à consulter selon une fréquence raisonnable ces outils de communication et à en gérer le contenu.

2. Cadre applicable à l'usage privé

L'usage à titre privé des outils de communication est toléré à condition que cet usage soit occasionnel, qu'il n'entrave en rien la productivité de l'utilisateur ni le bon fonctionnement du système d'information.

Rappel : Chaque message privé doit être identifié par le terme « Privé ». A défaut, les documents ou messages sont présumés avoir un caractère pédagogique.

B. Internet

L'utilisation d'Internet doit être appropriée et compatible avec l'activité pédagogique de l'utilisateur. Seuls les sites Internet présentant un lien direct et nécessaire au regard des activités pédagogiques, ont vocation à être consultés. Une consultation de sites Internet à des fins personnelles est tolérée à condition qu'elle soit ponctuelle et raisonnable.

Il est interdit d'utiliser l'accès à Internet du système d'information pour :

- télécharger, consulter des sites à caractère pornographique jugés illicites (pédophile, négationniste, extrémiste, raciste, xénophobe, violent ou contraire aux bonnes mœurs ou à l'ordre public…) ;
- consulter des sites prônant la discrimination sur la base du sexe, de l'orientation sexuelle, du handicap, de la religion et des convictions politiques, révisionnistes ou dont le contenu est susceptible de porter atteinte à la dignité d'autrui, à l'image ou formulant des propos diffamatoires, injurieux, malveillants, menaçants, provocants, calomnieux ou heurtant la sensibilité ;
- diffuser ou télécharger des œuvres protégées par des droits d'auteur ;
- participer à des jeux ou des paris en ligne.

Le service informatique se réserve le droit de bloquer l'accès Internet ou aux sites dont le contenu est jugé illégal ou présenterait un risque important pour la stabilité du réseau, de mettre en place des dispositifs de filtrage de sites illicites.

4) RESPONSABILITES, SANCTIONS

Le non-respect des règles énoncées par la Charte est passible des sanctions disciplinaires prévues par le Règlement intérieur et peut se voir interdire l'utilisation du matériel, de la connexion et des services mis à disposition par le Groupe. Selon la nature du manquement (imprudence, négligence, malveillance), l'utilisateur peut également voir sa responsabilité civile ou pénale engagée.
Le Groupe peut appeler en garantie un utilisateur pour les dommages et intérêts que le Groupe devrait éventuellement supporter en raison des agissements de ce dernier.