VERSION ELEVE

CHARTE D'UTILISATION DES MOYENS INFORMATIQUES ET DES OUTILS NUMÉRIQUES

INSTITUTION
Sévigné Saint-Louis

Table des matières

PREAMBULE

L'établissement s'efforce d'offrir à ses élèves les meilleures conditions de travail, notamment avec l'outil informatique : matériel, logiciels, réseau interne et internet. Son usage participe à la formation de l'élève ainsi qu'à l'action pédagogique des enseignants. Chaque étudiant dispose d'un droit d'utilisation des services proposés par l'établissement. Toutefois, l'ampleur de l'équipement et la complexité de sa gestion supposent de la part de chacun le respect du matériel et de certaines règles de fonctionnement. Le non-respect de ces règles peut nuire gravement au travail de chacun. Pour le confort de tous, le respect de cette charte et du règlement intérieur est une obligation qui s'impose à chaque utilisateur de l'informatique.

L'établissement utilise des techniques de protection pour empêcher l'utilisateur d'accéder à des informations illégales ou non destinées à un jeune public.

L'établissement peut procéder à des contrôles réguliers ou occasionnels pour vérifier que le réseau est utilisé dans le respect des règles établies. Les étudiants sont donc informés qu'en cas de comportement douteux, le responsable du réseau peut à tout moment vérifier les journaux d'accès à internet et savoir quels sites ont été visités et par quel utilisateur. Ces contrôles ne remettent pas en cause la confidentialité de la messagerie. L'établissement garantit également à l'utilisateur la protection des données à caractère personnel.

RAPPEL DE LA LEGISLATION

En matière de propriété intellectuelle : La protection de la propriété intellectuelle et des droits des auteurs impose qu'il soit interdit de copier, d'échanger et de diffuser de la musique, des vidéos, des logiciels, des jeux vidéo ou toute autre œuvre de l'esprit depuis le réseau de l'établissement.

En matière de droits de la personne : le respect des droits de la personne et de l'enfant impose qu'il soit interdit d'utiliser le réseau informatique pour véhiculer des injures ou d'une manière générale porter atteinte à l'honneur et à la vie privée d'autrui (interdiction de diffuser de fausses informations concernant autrui et de divulguer des renseignements d'ordre personnel).

Cette charte a pour objectifs d'informer l'utilisateur sur :

- Les usages permis des moyens informatiques mis à sa disposition ;
- Les règles de sécurité en vigueur ;
- Les mesures de contrôle prises par l'établissement ;
- Les sanctions éventuellement encourues par l'utilisateur ;
- De formaliser les règles générales de sécurité que l'utilisateur s'engage à respecter, en contrepartie de la mise à disposition des systèmes d'information et des équipements informatiques, et ainsi de déterminer les droits et devoirs des utilisateurs.

LEXIQUE

Charte informatique : La Charte définit les conditions générales d'utilisation de l'internet, des réseaux et des services multimédias au sein de l'établissement scolaire ou de l'école, en rappelant l'application du droit et en précisant le cadre légal afin de sensibiliser et de responsabiliser les utilisateurs.

Système d'information : Le système d'information (SI) est un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information au sein de l'Institution Sévigné Saint-Louis.

L'établissement : Représente le groupe scolaire Sévigné Saint-Louis.

Utilisateurs : Est considéré comme utilisateur, toute personne ayant accès aux ressources informatiques de l'Institution Sévigné Saint-Louis.

Il s'agit notamment des élèves des niveaux allant de la 6ème à l'enseignement supérieur de la section BTS.

Toutes personnes qui utilisent les ressources informatiques de l'Institution (Ordinateurs fixes & portables, Réseau Local, Réseau Internet, Logiciels, Equipements multimédia divers …).

Administrateurs : L'administrateur est une personne qui a la responsabilité de gérer les ressources informatiques de l'établissement. Il s'occupe de leurs mises à jour, de vérifier leurs bons fonctionnements et de créer les nouveaux comptes, configurer les autorisations et les fichiers à partager, les mails, le réseau, les sauvegardes, la sécurité...

Poste de travail : Le poste de travail désigne toute forme de terminal informatique (ordinateur, tablette, client léger…) capable d'accéder aux ressources de l'institution, permettant à l'utilisateur d'accomplir les tâches qui lui incombent.

Supports amovibles : Les supports amovibles sont des supports de données, qui, comme leur nom l'indique, peuvent être transférés d'un ordinateur à un autre. Ce sont typiquement les disques optiques, comme CD ou DVD, mais aussi les disques durs externes, les clés USB ou autres.

Journaux / Log : Tout événement de connexion depuis ou à destination du réseau de l'institution. Exemple : Pages Web consultées au fur à mesure de la journée. *(La loi oblige toute entreprise de disposer des journaux de connexion)*

Pare-feu : Un pare-feu est un système de sécurité de réseau informatique qui limite le trafic Internet entrant/sortant et interne à l'institution

ANSSI : L'ANSSI est l'autorité nationale en matière de sécurité et de défense des systèmes d'information.

CHAMP D'APPLICATION

Personnes visées au sein de l'Institution Sévigné Saint-Louis

Les obligations décrites dans la présente charte s'appliquent à toute personne qui utilise le système d'information de l'établissement. Il en est ainsi, notamment, des élèves ayant obtenu des droits personnels d'utilisation.

Accès par des tiers aux systèmes d'information

Tout utilisateur extérieur à l'institution ne peut avoir accès aux systèmes d'information que moyennant une autorisation expresse préalable délivrée par l'administrateur et il s'engage, dès lors, à respecter l'ensemble des dispositions de la présente charte.

Moyens informatiques et de communication électronique concernés

La présente charte concerne l'ensemble des moyens informatiques et de communication électronique qui sont mis à la disposition des utilisateurs à des fins scolaires exclusivement, ainsi que l'ensemble des moyens informatiques et de communication électronique qui sont la propriété personnelle de l'utilisateur, et pour lesquels celui-ci a obtenu une autorisation d'utilisation dans le cadre de son activité scolaire.

Les systèmes d'information et de communication de l'institution sont notamment constitués des éléments suivants :

- Ordinateurs portables ou fixes,
- Périphériques amovibles,
- Réseaux informatiques (serveurs, routeurs, commutateurs, bornes WIFI, firewall),
- Photocopieurs,
- Téléphones (fixes et portables) et smartphones,
- Tablettes électroniques,
- Logiciels,
- Fichiers informatiques et bases de données,
- Espaces de stockage individuel
- Messagerie,
- Connexions internet, intranet, extranet.

Dérogation possible

Toute demande de dérogation aux différents éléments définis dans le cadre de la présente Charte doit être présentée par écrit au responsable informatique. La décision finale est ensuite prise en concertation avec la Direction qui se réserve le droit d'accepter ou de refuser les demandes de dérogation.

USAGE DU SYSTEME D'INFORMATION ET OUTILS INFORMATIQUES

Usage des postes de travail

Les utilisateurs s'engagent à prendre soin du matériel, éteindre convenablement (PC & Système de vidéo-projection quand ils ne sont plus utilisés, le soir et aux intercours), et prévenir l'administrateur s'il y a une défaillance sur le matériel et les logiciels.

Modalités de fonctionnement de compte d'accès au réseau

L'établissement met à disposition des élèves des comptes utilisateurs personnels afin de s'authentifier sur le réseau interne de l'établissement et d'exploiter différentes ressources.

Les utilisateurs bénéficient également sur la durée de validité de leurs comptes utilisateurs d'un abonnement Microsoft 365 Education A1 qui leur permet d'utiliser la version Online de la suite bureautique Office hors de l'établissement.

Les utilisateurs s'engagent à n'utiliser cet abonnement Microsoft 365 uniquement à titre personnel.

Les utilisateurs s'engagent à ne pas divulguer leurs informations de connexion. De même, ils s'engagent à ne pas tenter de prendre connaissance des informations de connexion des autres utilisateurs.

Afin de garantir une sécurité accrue de leurs comptes Microsoft 365 hors de l'établissement, il est conseillé aux utilisateurs de se rapprocher de l'administrateur pour activer la double authentification sur leurs comptes éducation Microsoft 365. *(Authentification renforcée via un smartphone)*

Temporalités des comptes d'accès au réseau

L'accès au réseau et à ses ressources est limité dans le temps. Il est défini à l'année avec reconduction tacite ou non et en tout état de cause ne peut dépasser la durée de scolarité des utilisateurs.

Espaces personnels

Les utilisateurs disposent d'un espace de stockage personnel sur le réseau informatique de l'établissement et dans le cloud via l'ENT EcoleDirecte et le service de stockage Microsoft OneDrive, l'utilisateur s'engage à ne pas usurper l'identité d'un autre utilisateur pour accéder à ses données, ni les modifier, ni les supprimer.

L'utilisateur est seul responsable de l'enregistrement de ses fichiers.

Attention : Les répertoires de stockage des élèves seront supprimés tous les ans en fin d'année scolaire.

Espaces collaboratifs sur l'ENT EcoleDirecte

Les élèves disposent d'un espace de travail collaboratif créé dynamiquement par classe sur l'ENT EcoleDirecte. Ils s'engagent à respecter les préconisations d'usage des professeurs référents.

Droit de sortie du matériel informatique

L'établissement interdit strictement de sortir du matériel informatique des locaux.

Accès aux salles informatiques

Les utilisateurs ont accès aux salles informatiques dans le cadre des cours ou au CDI pendant les heures de permanence. Des étudiants peuvent néanmoins être admis dans une salle en dehors des heures de cours, mais toujours sous le contrôle d'un enseignant ou d'une personne étant à même d'assurer efficacement la surveillance.

UTILISATION ET PROTECTION DES DONNEES DE « FICHIERS »

Règles de stockage

L'utilisateur s'engage à sauvegarder ses données sur le serveur de fichier ou/et un espace de stockage Cloud validé par l'institution.

L'utilisateur s'engage à ne rien enregistrer directement sur les postes de travail.

Plusieurs espaces de stockage sont disponibles dans l'établissement :

- Cloud ENT EcoleDirecte
- Cloud Microsoft OneDrive
- Serveur de fichier local

Règles de sauvegarde des données

Les données se trouvant sur les serveurs de fichier sont sauvegardées toutes les nuits pour une durée de rétention de 30 jours.

Cas d'usage : Si vous avez supprimé par erreur un document enregistré sur votre espace de stockage personnel ou partagé, vous avez jusqu'à 30 jours pour demander à l'administrateur la restauration du document en question.

Supports amovibles

L'institution Sévigné déconseille fortement l'utilisation de supports amovibles tels que les clés USB ou disque dur externe. Les supports amovibles seront interdits à partir du 1er septembre 2023.

Les élèves devront utiliser les solutions de stockage que propose l'établissement (EcoleDirecte & OneDrive pour le Cloud) ou le serveur de fichier en local.

Données personnelles à caractère sensible

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.

L'institution 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.

REGLE D'USAGE DE LA SECURITE INFORMATIQUE

Rôle et responsabilités de l'établissement

L''institution s'engage à mettre tous les moyens en sa possession afin d'être en conformité envers les bonnes pratiques de sécurité défini par l'ANSI. (Stratégie de mot de passe, Sauvegarde, Mises à jour régulières des composants du SI, Anti-Spam, Antivirus)

L'établissement s'efforce dans la mesure du possible de maintenir accessible les services qu'il propose de manière permanente, mais n'est tenu à aucune obligation d'y parvenir. L'établissement peut donc interrompre l'accès, notamment pour des raisons de maintenance et de mise à niveau, ou pour toutes autres raisons, notamment techniques, sans qu'elle puisse être tenus pour responsable des conséquences de ces interruptions aussi bien pour l'utilisateur que pour tous tiers. L'établissement s'engage dans la mesure du possible, à tenir les utilisateurs informés de la survenance de ces interruptions.

Rôle et responsabilités des utilisateurs

L'élève/l'étudiant s'engage à :

- S'authentifier de manière nominative sur les postes de travail de l'établissement (hors cas particuliers)
- Ne pas ouvrir les pièces jointes reçues de l'extérieur quand l'émetteur du message est inconnu ou quand le contenu semble suspect ;
- Utiliser des mots de passe qui respectent les bonnes pratiques en vigueur ;
- Ne pas modifier la configuration de son poste de travail informatique effectuée par l'administrateur, que ce soit par adjonction, suppression ou modification ;
- Ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux à travers les matériels dont il a usage ;
- Ne pas mettre en évidence ces identifiants de connexion (Exemple : sur le bureau, écran, clavier …). Être prudent lors de la saisie de ses identifiants
- Ne pas divulguer les mots de passe du Wifi s'il en ont les droits d'utilisation. (Uniquement l'enseignement supérieur).
- Ne pas chercher à connecter son smartphone sur le réseau de l'institution s'il n'en pas reçu la permission
- Ne pas utiliser [même avec leur accord) où tenter d'utiliser des comptes autres que ceux qui lui sont attribués où masquer son identité ;
- Ne pas sortir les équipements informatiques de l'établissement.
- Ne pas détériorer le matériel.
- Ne pas télécharger de fichiers, en particulier médias, sans rapport avec l'activité scolaire ou présentant un risque pour le système d'information ;
- Verrouiller son ordinateur dès qu'il quitte son poste de travail
- Inscrire son usage des services du SI de l'institution dans le cadre de la réglementation en vigueur en matière de prévention des troubles de l'ordre public (respect de la propriété littéraire et artistique, respect des lois sur l'informatique et les libertés, respect de la vie

privée, respect de l'honneur et de la réputation, protection des mineurs, neutralité religieuse, politique et commerciale…), respect des données à caractère sensible.

Economie d'énergie

L'utilisateur s'engage à éteindre son poste de travail et le matériel audio-visuel aux intercours et en fin de journée (week-end, vacances scolaires).

Stratégie de sauvegardes

L'utilisateur s'engage à ne pas sauvegarder ses données sur les postes de travail mais uniquement sur le serveur de fichier ou sur un espace cloud approprié et validé par l'institution (ENT EcoleDirecte & OneDrive).

Uniquement les données situées sur le serveur de fichier sont sauvegardées (Données des espaces personnels).

Uniquement les OneDrive du personnel administratif sont sauvegardés.

Droit de licences et logiciels

L'utilisateur s'engage à ne pas pirater ou installer un logiciel qui n'aurait pas été validé par l'administrateur. Le téléchargement et l'installation d'applications tierces sont strictement interdits.

Messagerie

Le système de communication de référence mis à disposition des utilisateurs au sein de l'institution est la messagerie intégrée à l'ENT EcoleDirecte.

Usage des réseaux sociaux

L'institution se veut vigilante quant à l'usage des réseaux sociaux. Son usage est toléré uniquement dans un cadre éducatif et professionnel pour les étudiants de l'enseignement supérieur.

USAGE DE L'INTERNET & MESURES DE CONTROLE

Contrôle automatique

L'usage de la navigation internet au sein de l'institution Sévigné est encadré par des restrictions de navigation via des pare-feu.

Un contrôle automatique est mis en place via le pare-feu sur certaines applications, le web, les messageries, la connexion distante, les fichiers, afin d'identifier les utilisateurs, éviter les suppressions, diminuer les risques.

Le pare-feu vérifie et filtre tout le trafic sortant de l'établissement, aussi bien local que distant. Il vérifie également le trafic entrant.

A travers les journaux de connexion, il détient toutes les traces de l'activité qui transite par lui s'agissant :

- **De la navigation sur Internet :** sites visités, heures des visites, éléments téléchargés et leur nature (textes, images, vidéos ou logiciels) ;
- **Des messages envoyés et reçus :** expéditeur, destinataire(s), objet, nature de la pièce jointe *(et éventuellement texte du message)*.

Il filtre les URL des sites non autorisés par le principe de la liste noire. Les catégories des sites visés sont les sites diffusant des données de nature pornographique, pédophile, raciste ou incitant à la haine raciale, révisionniste ou contenant des données jugées comme offensantes, les jeux vidéo, les jeux d'argent, les sites contenant du code malveillant.

L'institution est dans l'obligation légale de disposer d'un outil d'enregistrement des journaux de connexion afin, si besoin exceptionnel, les transmettre aux autorités (gendarmes, …) en cas de plainte, de doute ou d'enquête.

L'administrateur n'est pas habilité à les consulter, hors cas particulier, pour des contrôles manuels.

Conformément à la loi les connexions sur les services administratifs et bancaires ne sont pas déchiffrés par le pare-feu.

Contrôle manuel

Des contrôles manuels peuvent être effectués par l'administrateur uniquement dans le cadre d'un dysfonctionnement et, de ce fait, il peut être amené à vérifier les opérations effectuées par les élèves afin de corriger une mauvaise manipulation.

Exemple : L'utilisateur ne parvient pas à accéder à une URL qui est censée être autorisée.

SANCTION

Le non-respect de l'une de ces règles entraînera des sanctions progressives

☞ Avertissement de l'utilisateur concerné

☞ Interdiction momentanée d'accès à l'outil informatique en dehors des impératifs fixés par les cours

☞ Interdiction permanente d'accès à l'outil informatique en dehors des impératifs fixés par les cours

☞ Rapport disciplinaire

☞ Mesure d'exclusion

☞ Poursuites pénales en cas d'infraction à la loi

Nous certifions avoir pris connaissance de l'ensemble des dispositions de la « charte multimédia ».
Nous les acceptons sans réserve et nous nous engageons à les respecter pleinement.