Collège & Lycée Privés
BELSUNCE
13, rue Fauchier
13002 Marseille

Téléphone : 04.91.90.51.14
Portable : 06.22.28.88.59
E-mail : collegelycee.belsunce13@sfr.fr

Année scolaire 2022/2023

CHARTE INFORMATIQUE

1. Champs d'application de la Charte

Les règles et obligations ci-dessous énoncées s'appliquent à toute personne autorisée (élève, enseignant, personnel administratif ou technique) utilisant les ordinateurs du collège et lycée polyvalent privés BELSUNCE nommé « l'établissement ».

2. Mission de l'administrateur

Sous la responsabilité du chef d'établissement, l'administrateur gère la mise en place, l'évolution et le fonctionnement du réseau (serveur, câblage, stations,...) et son administration (comptes utilisateurs, droits, logiciels, ...). L'administrateur a le droit de faire tout ce qui est nécessaire et autorisé par la loi pour assurer le bon fonctionnement des moyens informatiques de l'établissement. Il informe, les utilisateurs de toute intervention susceptible de perturber ou d'interrompre l'utilisation habituelle des moyens informatiques.

3. Conditions d'accès

Les services offerts par le réseau (stockage, courrier, accès Intranet et Internet, ...) sont destinés à un usage pédagogique, éducatif et administratif dans le cadre de la vie de l'établissement et du système éducatif ; l'utilisateur s'engage à en effectuer une utilisation rationnelle et loyale afin d'en éviter leur détournement à des fins personnelles. Chaque élève demandera l'autorisation aux responsables avant toute utilisation du réseau. L'administrateur attribuera un identifiant et un mot de passe à chaque utilisateur lui permettant de :

- se connecter au réseau de l'établissement,
- accéder aux informations et ressources pédagogiques présentes sur les réseaux Intranet et Internet et les utiliser,
- accéder à un espace de travail fourni par l'établissement.

Cet identifiant et ce mot de passe sont strictement personnels et confidentiels : ils donnent les droits aux utilisateurs suivant leur fonction dans l'établissement.

Chaque utilisateur est responsable de l'usage qu'il en fait : la communication à des tiers de ces informations, engage son entière responsabilité (cf. paragraphe 6).

L'administrateur n'ouvre de compte qu'aux utilisateurs ayant pris connaissance et signé le présent document, mais peut aussi le bloquer si l'utilisateur viole les règles énoncées.

4. Respect des règles de la déontologie informatique

L'élève est sous la responsabilité du professeur ou du personnel administratif qui supervise l'utilisation de l'outil informatique.

Chaque utilisateur s'engage à respecter les règles de la déontologie (notamment celles de la CNIL) et à **ne pas effectuer d'opérations qui pourraient avoir pour conséquence :**

- de masquer sa véritable identité (notamment dans les messages électroniques),
- **de s'approprier le mot de passe du compte d'autrui,**
- d'altérer les données ou d'accéder à des informations appartenant à d'autres utilisateurs du réseau sans leur autorisation,
- ***de porter atteinte à l'intégrité d'un utilisateur ou à sa sensibilité, notamment par l'intermédiaire de messages, textes ou images provocants,***
- d'interrompre le fonctionnement normal du réseau ou d'un des systèmes connectés (ou non) au réseau,
- de modifier ou de détruire des informations sur un des systèmes connectés au réseau,

De plus, l'utilisateur s'engage aussi à :

- ne pas se connecter ou essayer de se connecter sur un site sans rapport avec la recherche demandée par le professeur ou le personnel administratif,
- **utiliser Internet uniquement pour des tâches d'ordre pédagogique** (sont interdits notamment les "chats", weblogs, les sites "adultes" et "warez",...),
- **utiliser uniquement l'espace de travail fourni par l'établissement** ("webmail" personnel interdit), il ne doit en aucun cas l'utiliser pour l'envoi massif de mail à de multiples destinataires,
- n'imprimer que le strict nécessaire en noir et blanc (**préférer l'impression dans un fichier PDF**),
- ranger son poste de travail et sa chaise,
- ne pas boire, ni manger dans les salles (raisons de sécurité, de propreté et d'hygiène).
- L'utilisateur :
- **ne peut pas installer de logiciel sur un ordinateur, ou le rendre accessible sur le réseau qu'après accord de l'administrateur,**
- **s'interdit de faire des copies des logiciels autres que ceux qui, étant libres et/ou gratuits, sont à disposition sur les serveurs de l'établissement, rubrique ressources pédagogiques, logiciels libres, gratuits.**
- **Préférer la sauvegarde par envoi dans la boite mail que sur clé USB…..**

Il ne devra en aucun cas :

- **installer des logiciels à caractère ludique,**
- contourner les restrictions d'utilisation d'un logiciel,

- développer, copier et insérer dans le réseau des programmes de type “virus”, “ver” ou “cheval de Troie”,…
- stocker et/ou télécharger **des fichiers dont il ne détient pas les droits** dans son espace personnel,
- dégrader le matériel mis à sa disposition,

Un utilisateur ne doit jamais quitter un poste de travail sans se déconnecter (Démarrer – Déconnexion sur les postes Windows), sinon son répertoire personnel reste accessible pour tout utilisateur !

Toutes les activités des postes informatiques (utilisateur, date, heure, accès Internet, impressions, …) sont sous le contrôle permanent du serveur pédagogique et y sont stockées.

5. Utilisation équitable des moyens informatiques

Chaque utilisateur s'engage à prendre soin du matériel et des locaux informatiques mis à sa disposition. **Il informe l'administrateur réseau (par l’intermédiaire des professeurs et/ou correspondants informatique) de toute anomalie constatée.**

Chaque utilisateur respectera les normes d’utilisation et règles d’usage du serveur du réseau d’établissement afin de bénéficier de son environnement numérique de travail dans l'enceinte de l’établissement : zone privée « mes documents » **limitée à 20 Moctets (200 Mo pour le personnel de l’établissement),** pas d'activités risquant d'accaparer fortement les ressources informatiques (impression de gros documents, calculs importants, utilisation intensive du réseau,...) aux moments qui pénalisent le plus la communauté.

L'utilisateur qui contreviendrait aux règles précédemment définies s'expose à son exclusion du réseau, ainsi qu'aux sanctions et poursuites pénales prévues par les textes législatifs et réglementaires en vigueur ci-après.

6. Textes législatifs et réglementaires

- Circulaire « neutralité commerciale » N° II-67-290 du 3 juillet 1967 et N° 76-440 du 10 décembre 1976
- Loi « informatique et liberté » N°78-17 du 6 janvier 1978 modifiée par la loi N°2004-801du 6 août 2004 et la directive Européenne 95/46/CE du 24 octobre 1995
- Loi sur l'accès aux documents administratifs N°78-753 du 17 juillet 1978
- Loi « liberté de la presse » du 29 juillet 1881 et du 29 juillet 1982
- Loi sur la protection des logiciels du 3 juillet 1985
- Loi de la communication audiovisuelle N°86-1067 du 30 septembre 1986
- Loi relative à la fraude informatique N°88-19 du 5 janvier 1988
- Loi d’orientation sur l’éducation N°89-486 du 10 juillet 1989
- Loi « relative à la discrimination » N° 90-615 du 13 juillet 1990
- Circulaire « publication » N° 91-051 du 6 mars 1991
- Loi « relative au secret des correspondances » N° 91-646 du 10 juillet 1991
- Loi sur le code de la propriété intellectuelle du 1 juillet 1992
- Arrêter « base élèves » du 22 septembre 1995.
- Circulaire « chaine d’alerte » n° 2004-035 du 18 février 2004

Sanctions pénales **: Extraits de la loi du 27 mars 2012 relative à la fraude informatique, dite Loi Godfrain modifiée : Article 323-1 :** Modifié par LOI n°2012-410 du 27 mars 2012 - art. 9. Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende. Lorsqu’il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende. Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 75 000 € d'amende.**+ Articles : 323-2 + 323-3 + 323-4 + 323-5 + 323-6.** ***Article 323-7 :*** La tentative des délits prévus par les articles 323-2 à 323-6-1 est punie des mêmes peines.

⚠ En tant que parent, je sais que je suis responsable de tout ce que fait mon enfant sur les réseaux sociaux et m’engage à vérifier régulièrement qu’aucun texte, qu’aucune photo,… ne portera atteinte à qui que ce soit.

A Marseille, vu et pris connaissance le _____

L’utilisateur

NOM & Prénom _____

Pour les élèves Classe _____

La Directrice L’Utilisateur Les Parents