



## Charte d'utilisation des moyens Informatiques pour les élèves du Lycée Jean Mermoz

La charte informatique a pour objectif d'informer les élèves des règles qui s'imposent quant à l'utilisation d'un système d'information et l'exploitation de ses ressources. Elle permet aussi de fixer de manière transparente les conditions dans lesquelles la responsabilité des élèves peut être mise en cause.

### **1. Préambule**

Le Lycée franco-argentin Jean Mermoz met à disposition de ses élèves un système d'information (SI) et des moyens informatiques nécessaires à son activité, comprenant notamment un réseau informatique ainsi que des outils mobiles.

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

Dans un but de transparence à l'égard des élèves, 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.

Cette charte a pour objectif :

- De sensibiliser les élèves aux risques liés à la sécurité informatique en matière de libertés et de vie privée, notamment à travers les traitements de données à caractère personnel qu'ils sont amenés à effectuer ;
- D'informer les élèves 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 ;
- De formaliser les règles générales de sécurité que les élèves s'engagent 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 élèves.

## 2. Droits et devoirs

### 2.1. Droits

Les élèves ont le droit :

- d'accéder aux ressources numériques mises à disposition par l'établissement (ordinateurs, tablettes, logiciels pédagogiques, internet...).
- d'utiliser les services en ligne de l'école (messagerie, espace de travail, plateformes éducatives) dans le cadre des activités pédagogiques.
- d'être accompagnés et formés à un usage responsable et sécurisé du numérique.
- Voir leur vie privée respectée, notamment en ce qui concerne leurs données personnelles et la confidentialité de leurs travaux scolaires.
- de travailler dans un environnement numérique sécurisé, protégé des contenus inappropriés et des cybermenaces.
- d'exprimer des besoins ou signaler des incidents (matériel défectueux, cyberharcèlement, difficultés d'accès, etc.).
- d'accéder à leurs productions numériques et de conserver leurs travaux scolaires.

### 2.2. Devoirs

Les élèves s'engagent à :

1. Utiliser les outils numériques uniquement à des fins scolaires, dans le respect du cadre défini par les enseignants et l'établissement.
2. Protéger leurs identifiants et mots de passe : ne pas les partager, ne pas usurper l'identité d'autrui.
3. Respecter les règles de sécurité informatique (ne pas contourner les filtrages, ne pas installer de logiciels non autorisés, ne pas modifier les configurations).
4. Adopter un comportement responsable en ligne : respect d'autrui, politesse, absence de harcèlement ou de propos discriminatoires.
5. Respecter la loi sur les droits d'auteur : ne pas copier, pirater, diffuser du contenu protégé.
6. Ne pas accéder, transmettre ou stocker de contenus choquants, illégaux ou inappropriés.
7. Respecter l'intégrité du matériel informatique : utiliser le matériel avec soin, signaler toute panne ou incident.
8. Ne pas réaliser de photos, de vidéos ou d'enregistrements sans autorisation des personnes concernées et de l'établissement.
9. Signaler immédiatement toute situation mettant en danger la sécurité numérique ou l'intégrité des données.

## 3. Champ d'application

### 3.1. Utilisateurs concernés

Sauf mention contraire, la présente charte s'applique à l'ensemble des élèves utilisateurs du système d'information et de communication du Lycée Jean Mermoz

### 3.2. Système d'information et de communication

Le système d'information et de communication du Lycée Jean Mermoz est notamment constitué des éléments suivants : ordinateurs (fixes ou portables), périphériques y compris clés USB, réseau informatique (serveurs, routeurs et connectique), photocopieurs, télécopieurs, tablettes, logiciels, fichiers, données et bases de données, système de messagerie, connexion internet, intranet, extranet.

## 4. Confidentialité

### 4.1. Paramètres d'accès

L'accès à certains éléments du système d'information (comme la messagerie électronique, 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).

L'utilisation des systèmes informatiques a pour objet exclusif de mener à bien des activités d'enseignement et de documentation.

Chaque élève se voit attribuer un identifiant et un mot de passe qui lui permettent d' :

- Accéder aux ressources informatiques et pédagogiques mise à disposition par l'établissement.
- Accéder aux informations et ressources présentes sur Internet.

**Cet identifiant et ce mot de passe sont strictement personnels et confidentiels.**

L'établissement met également à disposition des élèves des logins dits « génériques » permettant l'utilisation des salles pédagogiques. Dans le cadre de son activité, l'élève qui utilise un poste informatique reste responsable de l'usage qu'il fait du matériel même s'il ne dispose pas d'un login nominatif et personnel. L'identification éventuelle pouvant être effectuée aux moyens des historiques des événements de l'ordinateur par exemple. De plus l'élève qui se connecte via un compte générique doit s'assurer qu'il ne laisse pas d'informations personnelles sur le poste (fichiers ou sessions personnelles ouverts ...).

## **4.2. Données**

L'élève reste vigilant quant au risque de divulgation d'informations personnelles ou appartenant à l'établissement lorsqu'il utilise des outils informatiques.

Aucune donnée confidentielle (documents internes, identifiants, informations sur les élèves ou le personnel) ne peut être partagée avec des personnes ou services non autorisés.

La collecte, la copie ou la diffusion de données issues du système d'information s'effectue uniquement dans un cadre pédagogique validé par l'équipe éducative.

Le droit à l'image s'applique pleinement : aucune photo, vidéo ou enregistrement d'une personne présente dans l'établissement ne peut être publié ou transmis sans son autorisation et celle de l'école.

## **5. Sécurité**

### **5.1. Rôle de l'Établissement**

L'établissement met en œuvre les moyens humains et techniques appropriés pour assurer la sécurité matérielle et logicielle du système d'information et de communication. À ce titre, il lui appartient de limiter les accès aux ressources sensibles et d'acquiescer les droits de propriété intellectuelle ou d'obtenir les autorisations nécessaires à l'utilisation des ressources mises à disposition des élèves.

Le service informatique veille à l'application des règles de la présente charte. Il est assujéti à une obligation de confidentialité sur les informations qu'il est amené à connaître.

### **5.2. Responsabilité de l'élève**

L'élève est responsable quant à lui des ressources qui lui sont confiées. Il concourt à la protection des dites ressources, en faisant preuve de prudence et de vigilance. En particulier, il signale au professeur en charge de la classe de toute violation ou tentative de violation de l'intégrité de ces ressources, et, de manière générale, tout dysfonctionnement, incident ou anomalie.

L'élève ne quitte pas son poste de travail et les postes en libre-service dont il a la responsabilité sans fermer la session, laissant ainsi des ressources ou services accessibles des supports informatiques (clé USB, CD-Rom...) contenant des données personnelles accessibles à quelqu'un d'autre.

L'élève n'installe pas ou ne supprime pas des logiciels, ne copie ni n'installe de fichiers susceptibles de créer des risques de sécurité au sein de l'établissement. Il n'est pas autorisé à modifier les paramètres de son poste de travail ou des différents outils mis à sa disposition, ni à contourner aucun des systèmes de sécurité mis en œuvre à l'établissement

Si un élève constate un dysfonctionnement, il alerte le professeur en charge à ce moment-là.

L'élève ne se connecte pas ou n'essaie pas de se connecter sur un site sans y être autorisé ou sur un site sans rapport avec la recherche demandée par le professeur

L'élève s'oblige en toutes circonstances à se conformer à la législation, qui protège notamment les droits de propriété intellectuelle, le secret des correspondances, les données personnelles, les systèmes de traitement automatisé de données, le droit à l'image des personnes.

### **5.3. Quelques bonnes pratiques à respecter**

- Toujours verrouiller son poste lorsque l'on ne l'utilise pas.
- Ne jamais confier son mot de passe d'identification à autrui
- Laisser des informations personnelles sur les postes est fortement déconseillé, d'autant plus si l'utilisateur est connecté sur un compte générique.
- Utiliser des supports amovibles (clef USB, disque dur USB...) est fortement déconseillé.
- Prêter attention aux mails reçus, ne pas cliquer sur un lien sans être sûr que l'expéditeur est une personne de confiance.

## **6. Internet**

### **6.1. Accès aux sites**

Un accès à Internet est attribué aux élèves afin de permettre la consultation des sites web. L'établissement met en œuvre des systèmes de filtrage afin d'interdire l'accès à certains sites dont le contenu lui semble illicite, en contradiction ou sans rapport avec ses objectifs éducatifs, ou requiert l'âge de la majorité. Ce filtrage est régulièrement mis à jour par l'établissement. Il peut toutefois y avoir un délai pour la détection et le blocage de nouveaux sites.

### **6.2. Autres utilisations**

La contribution des élèves à des forums de discussion, systèmes de discussion instantanée, chats, blogs n'est autorisée dans l'établissement qu'à titre pédagogique.

De même, tout téléchargement de fichier, en particulier de fichier média, est prohibé, sauf pour une utilisation pédagogique indiquée par le professeur.

Il est rappelé que les élèves ne doivent en aucun cas se livrer sur Internet à une activité illicite ou portant atteinte à l'image de l'établissement.

Ils sont informés que le service informatique enregistre leur activité sur Internet et que ces traces pourront être exploitées à des fins de statistiques, contrôle et vérification dans les limites prévues par la loi, en particulier en cas de perte importante de bande passante sur le réseau de l'établissement.

## **7. Messagerie électronique**

La messagerie électronique attribuée par l'établissement à l'élève doit être utilisée exclusivement dans le cadre d'une activité pédagogique.

Les messages électroniques reçus sur la messagerie font l'objet d'un contrôle antiviral et d'un filtrage anti-spam.

### **7.1. Conseils généraux**

Un message électronique peut être communiqué très rapidement à des tiers et 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.

Avant tout envoi, il est impératif de bien vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises.

Les élèves veillent au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne comportent pas d'éléments illicites, tels que des propos diffamatoires, injurieux, contrefaisants.

### **7.2. Limites techniques**

Le service informatique peut limiter la taille, le nombre et le type des pièces jointes pour éviter l'engorgement du système de messagerie. L'élève est tenu de supprimer lui-même dès que possible tous les messages inutiles.

Si l'élève quitte l'établissement (fin de cursus, départ dans un autre établissement...) la messagerie électronique sera suspendu au bout de 3 mois. Et au bout de 6 mois le compte sera supprimé de façon définitive.

Compte suspendu : Il sera possible de récupérer les informations en contactant le service informatique.

Compte supprimé : Le mail n'existe plus et les données liées au mail (Drive Sheet Doc etc....) sont effacés de façon définitive sans possibilité de récupération

### **7.3. Utilisation personnelle de la messagerie**

Les élèves sont invités, à utiliser leur messagerie personnelle via un client en ligne pour l'envoi de messages à caractère personnel plutôt que la messagerie de l'établissement.

## **8. Contrôle des activités**

### **8.1. Contrôles automatisés**

Le système d'information et de communication s'appuie sur des fichiers journaux ("logs"), créés en grande partie automatiquement par les équipements informatiques et de télécommunication. Ces fichiers sont stockés sur les postes informatiques et sur le réseau. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations de l'établissement, en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des élèves accédant au système d'information.

Les élèves sont informés que de multiples traitements sont réalisés afin de surveiller l'activité du système d'information et de communication. Sont notamment surveillées et conservées les données relatives :

- à l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications et suppressions de fichiers ;

- aux connexions entrantes et sortantes au réseau interne et à Internet, pour détecter les tentatives d'intrusion et les activités, telles que la consultation de sites ou le téléchargement de fichiers.

Dans le cadre de la maintenance informatique mais aussi d'activités pédagogiques ponctuelles, un logiciel de gestion et d'administration des ordinateurs permet la connexion à tout ordinateur identifié sur le réseau de l'établissement ainsi qu'une éventuelle prise en main à distance.

## **9. Information et sanctions**

La présente charte est affichée publiquement en annexe du règlement intérieur.

Chaque élève se conforme aux procédures et règles de sécurité édictées par le service informatique dans le cadre de la présente charte.

Sanctions :

Si les règles de la présente charte ne sont pas respectées, des sanctions seront appliqués en fonction de la gravité des faits :

- Les comptes pourront être suspendus sur décision de la direction
- L'établissement s'autorise à contrôler le contenu des échanges pouvant être faits par les moyens de communication de l'école en cas de signalement
- Des sanctions additionnelles seront appliquées proportionnellement à la gravité du non-respect de la présente charte

## **10. Entrée en vigueur**

La présente charte est applicable à compter du 01/03/2026

Elle a été adoptée après information et consultation du conseil d'établissement en date du 19 novembre 2025