



Unité Développement pédagogique
Unité Informatique et Statistiques

Réf. : 2025-08-D-25-fr-1

Orig. : EN

CHARTRE D'UTILISATION DES RESSOURCES ET DISPOSITIFS INFORMATIQUES PAR LES ÉLÈVES DE L'ÉCOLE EUROPÉENNE

Annexe au MEMO 2025-08-M-1

Table des matières

PRÉAMBULE.....	3
1. RESSOURCES ET DISPOSITIFS INFORMATIQUES.....	3
1.1 Définition	3
1.2 Règle d'or.....	4
1.3 Accès aux ressources et appareils informatiques	4
2. RÈGLES GÉNÉRALES DE BONNE CONDUITE.....	5
2.1 Commentaires généraux.....	5
2.2 Respect de la confidentialité	6
2.3 Respect du réseau et des postes de travail	6
2.4 Respect des droits de propriété intellectuelle	7
2.5 Respect des membres de la communauté scolaire et de l'École	7
3. RÈGLES PARTICULIÈRES D'UTILISATION D'INTERNET	8
3.1 Utilisation du réseau de l'École	8
3.2 Supervision et assistance pendant les sessions pour les élèves de l'École	8
3.3 Médias sociaux	9
3.4 Intelligence artificielle	9
4. RÈGLES PARTICULIÈRES CONCERNANT L'APPRENTISSAGE / L'ENSEIGNEMENT EN LIGNE.....	9
5. RAPPORT À L'ÉQUIPE ÉDUCATIVE/INFORMATIQUE.....	10
6. RESPONSABILITÉ	10
7. SANCTIONS PRÉVUES	10
8. RÉVISION	11



Schola Europaea

Bureau du Secrétaire général

Charte d'utilisation des ressources et dispositifs informatiques par les élèves des Écoles européennes

PRÉAMBULE

Les Écoles européennes s'efforcent d'offrir aux élèves les meilleures conditions de travail possibles en matière de services informatiques, numériques et multimédias. La présente Charte établit les règles de bon usage et de bonne conduite vis-à-vis des ressources informatiques à finalité pédagogique mises à leur disposition.

Cette Charte constitue une annexe au Règlement intérieur de l'École européenne (ci-après désignée par le terme « École ») et s'inscrit dans le cadre des lois et règlements en vigueur relatifs notamment au droit d'auteur, aux droits de propriété intellectuelle, à la protection de la vie privée (incluant notamment le droit à l'image) et au traitement des données à caractère personnel, ainsi qu'à la criminalité informatique.

1. RESSOURCES ET DISPOSITIFS INFORMATIQUES

1.1 Définition

« Ressources et dispositifs informatiques » : l'ensemble des dispositifs techniques et des services informatiques de l'École : *réseau, serveurs et postes de travail, tableaux blancs interactifs, périphériques (imprimantes, disques durs externes, etc.), ordinateurs portables, ordinateurs et tablettes, applications logicielles, identifiants et utilisation des services Internet de l'École ainsi que des ressources d'apprentissage numériques¹ fournies par cette dernière.*

¹ Conformément à la définition mentionnée dans la procédure d'approbation de l'utilisation d'une ressource pédagogique numérique dans les Écoles européennes (annexe au MEMO 2019-12-M-3/GM).

1.2 Règle d'or

Les ressources informatiques de l'École européenne sont destinées à être utilisées *uniquement* pour des activités pédagogiques.

1.3 Accès aux ressources et appareils informatiques

L'accès aux ressources et aux appareils fournis par l'École est un privilège, non un droit.

Chaque élève est tenu de respecter scrupuleusement les conditions de fonctionnement et les règles de bon usage et de bonne conduite contenues dans la présente Charte.

L'École peut effectuer des contrôles réguliers ou occasionnels pour vérifier que les ressources et appareils informatiques sont utilisés conformément aux dispositions de la présente Charte et se réserve le droit de révoquer ce privilège en cas de besoin.

Dans l'École, l'accès aux ressources et appareils informatiques est assuré sous la responsabilité de la direction de l'École et sous le contrôle d'un membre de l'équipe éducative.

L'École offre un accès à différentes ressources informatiques :

- aux ordinateurs de l'école par le biais d'un compte personnel (identifiants fournis),
- au réseau de l'École, y compris :
 - ☐ à des espaces de stockage sur les serveurs de l'école : à des espaces partagés ou limités à un compte personnel,
 - ☐ à des imprimantes en réseau,
- à des services en ligne Microsoft 365 (y compris notamment un service de courrier électronique/messagerie) géré par l'École européenne,
- à des logiciels propriétaires, sous licence ou à code source ouvert (open source),
- à Internet,
- au Wi-Fi de l'école sur un appareil personnel pour les élèves éligibles au BYOD (Apportez votre propre appareil).

Tous les comptes d'accès et les identifiants d'utilisateur fournis à l'élève sont personnels et ne peuvent être utilisés que par l'élève concerné. Ainsi, les codes d'accès et les identifiants doivent être absolument confidentiels et ne peuvent être divulgués à des tiers (à l'exception des représentants légaux de l'élève). Cependant, **il est strictement interdit aux représentants légaux des élèves d'utiliser les ressources informatiques mises à la disposition des élèves à d'autres fins que l'enseignement et l'apprentissage des élèves** (comme l'utilisation de la suite bureautique MS 365 pour des besoins personnels ou la participation à des réunions avec le compte de l'élève, etc.).

Avant de quitter leur poste de travail, les élèves doivent toujours s'assurer qu'ils se sont bien déconnectés.

L'élève informera son conseiller pédagogique s'il rencontre un problème avec son compte et en cas de perte, de vol ou de compromission de ses codes d'accès.

2. RÈGLES GÉNÉRALES DE BONNE CONDUITE

2.1 Commentaires généraux

Les élèves sont tenus de respecter les règles de bonne conduite lorsqu'ils utilisent les ressources et les appareils mis à la disposition de l'École à des fins pédagogiques. Ainsi, l'accès aux ressources par un élève qui utilise son appareil mobile personnel dans l'École (c'est-à-dire l'accès au réseau) ou à l'extérieur de l'École implique également le respect de cette Charte.

Pour un usage personnel en dehors de l'école, chaque élève recevra 5 licences d'installation Microsoft 365 pour les ordinateurs et/ou les smartphones et tablettes. Ces licences peuvent être utilisées et installées sur des appareils informatiques régulièrement utilisés par l'élève et protégés par un mot de passe dans le respect des règles générales de bonne conduite énoncées dans la présente Charte.

2.2 Respect de la confidentialité

Les élèves ont l'interdiction de :

- chercher à s'approprier le mot de passe d'autres personnes,
- se connecter avec les noms d'utilisateur et les mots de passe d'autres personnes,
- utiliser la session ouverte d'un autre utilisateur sans son autorisation explicite,
- ouvrir, divulguer/partager, modifier, télécharger ou supprimer les fichiers d'autres personnes et, plus généralement, essayer d'accéder à des informations leur appartenant sans leur permission,
- enregistrer un mot de passe dans un logiciel Internet, tel que Google Chrome, Internet Explorer, Firefox, etc., **lors de l'utilisation d'appareils non personnels.**

2.3 Respect du réseau et des postes de travail

Il convient de démontrer que les locaux et le matériel sont scrupuleusement respectés. Les claviers, souris et écrans d'ordinateur doivent être manipulés avec précaution. Ainsi, les élèves ne sont pas autorisés à manger et à boire lorsqu'ils utilisent des postes de travail dans l'école, afin de ne pas les endommager. Les élèves ne doivent pas bloquer délibérément les casiers avec des cadenas électroniques gratuits réservés au chargement des appareils BYOD (Apportez votre propre appareil).

Les élèves ont l'interdiction de :

- chercher à modifier la configuration de l'équipement (ordinateur portable, tablette, poste de travail),
- chercher à modifier ou à détruire les données du réseau ou du poste de travail,
- installer des logiciels ou de copier des logiciels présents sur le réseau,
- accéder à, ou de tenter d'accéder à des ressources autres que celles autorisées par l'École,
- ouvrir des messages, des fichiers, des documents, des liens, des images envoyés par des expéditeurs inconnus,
- insérer, dans quelque appareil que ce soit, un disque amovible, sans l'autorisation d'un adulte responsable,
- connecter un dispositif ou un support de stockage (USB, téléphone portable, autre) sans l'autorisation d'un adulte responsable,
- interférer délibérément avec le fonctionnement du réseau, notamment en utilisant des programmes conçus pour introduire des programmes malveillants ou pour contourner la sécurité (virus, logiciels espions ou autres),
- subvertir ou tenter de corrompre les systèmes de protection installés (pare-feu, programmes antivirus, etc.),
- utiliser des tunnels VPN².

² En informatique, un **Réseau privé virtuel, VPN** est un système permettant de créer un lien direct entre des ordinateurs à distance, en isolant ce trafic dans une sorte de tunnel.

2.4 Respect des droits de propriété intellectuelle

Les élèves ont l'interdiction de :

- télécharger ou faire des copies illégales de matériel (streaming, audio, films, logiciels, jeux, etc.) protégé par des droits de propriété intellectuelle, à moins que ce matériel ne soit mis à disposition sous une licence (telle que Creative Commons) qui autorise une telle utilisation,
- plagier, c'est-à-dire reproduire, (re)diffuser ou communiquer au public, sous quelque forme que ce soit et par quelque moyen que ce soit (tableaux, graphiques, équations, textes juridiques, images, textes écrits), tout contenu protégé par des droits de propriété intellectuelle (tels que le droit d'auteur). Ils doivent également citer leurs sources lorsqu'ils font référence aux hypothèses, théories ou opinions d'autrui.

L'utilisation d'informations trouvées sur Internet pour un travail en classe implique que les sources soient incluses et correctement citées par l'élève. L'élève peut demander l'assistance d'un des membres de l'équipe pédagogique à cet égard.

2.5 Respect des membres de la communauté scolaire et de l'École

Tous les élèves doivent utiliser les outils numériques dans le respect de la dignité, du bien-être et des droits de tous les membres de la communauté scolaire.

Les élèves ont l'interdiction de :

- afficher à l'écran et publier des documents ou participer à des échanges à caractère diffamatoire, injurieux, extrémiste, pornographique ou discriminatoire, qu'ils soient fondés sur l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'état de santé ou l'orientation sexuelle.
- intimider d'autres personnes (cyberintimidation³), que ce soit en leur nom propre ou en utilisant une fausse identité ou un pseudonyme. Les élèves sont encouragés à signaler toute cyberintimidation à un adulte de confiance ou à un membre du personnel, tandis que l'école soutiendra toutes les parties impliquées, en adoptant une approche réparatrice et éducative dans la mesure du possible.
- utiliser des listes d'adresses e-mail ou de données à caractère personnel d'autrui à des fins autres que celles prévues par les objectifs pédagogiques ou éducatifs, et conformément aux réglementations en matière de protection des données.
- utiliser un langage inapproprié dans les e-mails, les messages, les chats ou tout autre moyen de communication (l'auteur du message est seul responsable du contenu envoyé).
- porter atteinte à la réputation d'un membre de la communauté scolaire ou de l'École en diffusant des textes, des images et/ou des vidéos.
- conclure des contrats, vendre ou faire de la publicité de quelque manière que ce soit au nom de l'École, sauf si le projet a été préalablement approuvé par la direction de l'École.

³ La cyberintimidation comprend le harcèlement, les menaces, l'exclusion ou l'humiliation répétés ou intentionnels d'autres personnes par le biais de moyens numériques, tels que les messages, les médias sociaux, les images ou les vidéos.

3. RÈGLES PARTICULIÈRES D'UTILISATION D'INTERNET

3.1 Utilisation du réseau de l'École

L'accès à l'Internet au sein de l'École européenne est un privilège, pas un droit.

L'utilisation du réseau pédagogique basé sur Internet est exclusivement destinée à des activités d'enseignement et d'apprentissage correspondant aux missions des Écoles européennes.

Il est strictement interdit aux élèves de :

- se connecter à des services de chat en direct ou à des forums de discussion, sauf autorisation d'un membre de l'équipe pédagogique, à des fins pédagogiques, ou à des
- médias sociaux,
- partager des informations personnelles susceptibles de permettre l'identification d'une personne (prénom, nom, e-mail, adresse, etc.),
- accéder à des sites Internet à contenu pornographique ou faisant l'apologie de la haine, de la discrimination ou de la violence fondée sur la race, l'origine ethnique, la religion, l'orientation sexuelle ou d'autres caractéristiques personnelles, télécharger ou installer des logiciels ou des applications de quelque nature que ce soit.

Les élèves ne doivent en aucun cas mentionner leur nom, afficher une photo, mentionner leur adresse, leur numéro de téléphone ou toute autre information facilitant leur identification sur Internet et/ou les données personnelles de quelqu'un d'autre.

Il est strictement interdit aux élèves d'utiliser l'adresse e-mail liée à leur compte MS365 (...@student.eursc.eu) pour créer des comptes sur des applications, sites web ou logiciels non autorisés par un membre de l'équipe pédagogique ou par la Direction de l'École.

3.2 Supervision et assistance pendant les sessions pour les élèves de l'École

L'École utilisera un système de supervision et d'assistance pour soutenir l'engagement des élèves dans un processus d'apprentissage continu et pour permettre aux responsables du cours en question et au personnel de la bibliothèque d'aider les élèves directement depuis leur poste de travail.

Seules les personnes autorisées par la Direction de l'École peuvent utiliser le logiciel de supervision et d'assistance, et elles sont tenues de respecter la charte informatique applicable à leur fonction dans l'École.

Ce système permet :

- l'accès à distance aux écrans des élèves pour les aider et les maintenir concentrés sur leurs tâches,
- de rendre l'enseignement plus efficace, en affichant l'écran de la personne en charge de la leçon à toute la classe,
- de sélectionner les écrans des élèves pour présenter leur travail,
- de désactiver tous les écrans des élèves pour capter leur attention.

Aucun enregistrement de leur session ou de leur activité n'est effectué.

3.3 Médias sociaux

Il est interdit aux élèves de se connecter aux médias sociaux avec leur adresse e-mail liée à leur compte MS365 (...@student.eurisc.eu). **La réutilisation du mot de passe utilisé pour le compte MS365 dans d'autres systèmes, sites web et applications est strictement interdite.**

L'utilisation d'un appareil numérique privé (téléphone, tablette, ordinateur portable) ne dispense pas les élèves de suivre les règles de bon usage et de bonne conduite prévues par la présente Charte, en ce qui concerne le respect des membres de la communauté scolaire et de l'École. Les élèves restent responsables du contenu affiché.

3.4 Intelligence artificielle

L'intelligence artificielle (IA) désigne la capacité des systèmes informatiques à effectuer des tâches généralement associées à l'intelligence humaine, telles que l'apprentissage, le raisonnement, la résolution de problèmes, la perception et la prise de décision. L'IA générative peut traiter le contenu (analyser, transformer ou créer) sur la base des données fournies par l'utilisateur, généralement de manière conversationnelle.

- Les élèves ne peuvent accéder aux outils d'IA basés sur le web en utilisant leur adresse e-mail de l'école (...@student.eurisc.eu) qu'avec l'autorisation explicite de l'École. Si l'IA est utilisée en dehors de l'École pour des devoirs ou des projets, les élèves doivent rester honnêtes et transparents, conformément à la politique de l'École ou aux directives spécifiques au cours.
- Les élèves doivent utiliser les outils d'IA en toute responsabilité et conformément à la loi, en protégeant la vie privée et la confidentialité, en respectant la propriété intellectuelle, en étant responsables des contenus générés par l'IA qu'ils utilisent et en recourant à ces outils de manière réfléchie compte tenu de leur impact sur l'environnement.

4. **RÈGLES PARTICULIÈRES CONCERNANT L'APPRENTISSAGE / L'ENSEIGNEMENT EN LIGNE**

L'apprentissage ou l'enseignement en ligne nécessite le respect des règles de bon usage et de bonne conduite énoncées dans la présente Charte, que ce soit dans le cadre de :

- apprentissage mixte : l'apprentissage ou l'enseignement en ligne à l'École, l'utilisation de ressources numériques approuvées par la direction de l'École ou la réalisation d'activités asynchrones (par exemple, les devoirs) ;
- apprentissage à distance : lorsque les cours en ligne ont lieu pendant que l'École est fermée ;
- apprentissage hybride : lorsque certains élèves assistent aux cours en personne et que d'autres participent en ligne.

Les actions suivantes sont interdites :

- photographier et/ou filmer des enseignants ou des élèves participant à l'apprentissage en ligne à l'aide d'appareils personnels, et surtout publier de telles images ou vidéos,
- participer à des sessions d'apprentissage ou d'enseignement en ligne sans y avoir été expressément invité,
- inviter les siens à des sessions d'apprentissage ou d'enseignement en ligne sans l'accord de la personne qui organise la session,

- utiliser des ressources d'apprentissage numériques pour intimider, tyranniser, diffamer ou menacer d'autres personnes.

Le droit de contrôler l'utilisation de son image est reconnu à tous les membres de la communauté scolaire. En conséquence, l'École ne tolérera pas l'utilisation d'images ou de vidéos prises à l'insu ou sans le consentement des personnes concernées.

5. RAPPORT À L'ÉQUIPE ÉDUCATIVE/INFORMATIQUE

L'élève s'engage à signaler à un membre de l'équipe pédagogique et/ou informatique (conseiller pédagogique, coordinateur informatique, enseignant, etc.), dans les plus brefs délais :

- tout logiciel ou dispositif suspect,
- la perte, le vol ou la compromission de ses informations d'authentification,
- tout message, fichier, document, lien, image envoyée par un expéditeur inconnu.

6. RESPONSABILITÉ

Les dommages intentionnels causés aux appareils et aux ressources informatiques de l'École peuvent entraîner des frais de réparation pour les représentants légaux des élèves concernés, conformément à l'article 32 du Règlement général des Écoles européennes (2014-03-D-14).

Tout élève qui choisit d'apporter un téléphone portable ou un autre appareil numérique à l'École le fait à ses propres risques et est personnellement responsable de la sécurité de son téléphone portable ou de son appareil.

Sans préjudice des exceptions prévues lorsque les élèves sont tenus d'apporter un appareil à l'École dans le cadre d'un programme BYOD, l'école décline toute responsabilité en cas de perte, de vol, de dommage ou de vandalisme d'un téléphone ou de tout autre appareil, ou en cas d'utilisation non autorisée d'un tel appareil.

7. SANCTIONS PRÉVUES

Tout élève qui contrevient aux règles énoncées ci-dessus s'expose aux mesures disciplinaires prévues par le Règlement général des Écoles européennes (2014-03-D-14) et le Règlement intérieur de l'École ainsi qu'aux sanctions et poursuites pénales prévues par la loi.

Tous les membres de l'équipe éducative doivent s'engager à faire respecter ces dispositions par les élèves qui sont sous leur responsabilité et sont tenus d'exercer un contrôle rigoureux à cet égard.

L'administrateur des technologies de l'information doit constamment s'assurer, à sa satisfaction, que les ressources informatiques fonctionnent correctement et sont utilisées à bon escient. À cette fin, la surveillance des ressources et des appareils informatiques permet de détecter les anomalies (utilisation anormale du réseau, espace de stockage excessif, tentative de cyberattaque, etc.). Si des anomalies sont détectées, l'administrateur informatique se rapprochera de la direction de l'École pour convenir des mesures à prendre.

Toutefois, en cas d'urgence absolue et pour protéger le système informatique de l'école, l'administrateur informatique peut prendre la décision immédiate de bloquer l'accès informatique à un ou plusieurs élèves, puis en référer immédiatement à la direction.

Ce type d'intervention ne peut se faire que dans le respect d'objectifs clairement définis, à savoir :

- la prévention des actions illégales ou diffamatoires, des actions contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui.
- la protection des intérêts économiques ou financiers de l'École, auxquels la confidentialité est attachée,
- la sécurité et/ou le bon fonctionnement technique des systèmes informatiques, y compris la maîtrise des coûts y afférents, et la protection physique des installations de l'École,
- le respect en toute bonne foi des principes et des règles d'utilisation des technologies disponibles, ainsi que de la présente Charte.

8. RÉVISION

La présente Charte sera réexaminée au plus tard au cours de l'année scolaire 2027/28.