



École européenne de Bruxelles IV (Laeken)
European School of Brussels IV (Laeken)

POLITIQUE SCOLAIRE

CHARTRE D'UTILISATION DES RESSOURCES ET DISPOSITIFS INFORMATIQUES DES ÉLÈVES

CRÉATION : 01-09-2022

DERNIÈRE RÉVISION : 12-07-2022

VALIDATION : Approuvée lors de la réunion du SAC (23 juin 2022)

DIFFUSION : Communauté scolaire

Table des matières

1. Préambule.....	3
2. Ressources et dispositifs informatiques.....	3
2.1. Définition.....	3
2.2. Règle d'or.....	3
2.3. Access to IT resources and devices.....	3
3. Règles générales de bonne conduite.....	4
3.1. Remarques générales.....	4
3.2. Respect de la confidentialité.....	5
3.3. Respect du réseau et des postes de travail.....	5
3.4. Respect des droits de propriété intellectuelle.....	6
3.5. Respect des membres de la communauté scolaire et de l'École.....	6
4. Règles particulières pour l'usage d'Internet.....	7
4.1. Réseau de l'École.....	7
4.2. Supervision et assistance de la session des élèves dans l'École.....	7
4.3. Réseaux sociaux.....	8
5. Règles particulières concernant l'apprentissage / l'enseignement en ligne.....	8
6. Signalement à l'équipe éducative.....	9
7. Protection des données.....	9
8. Responsabilité.....	9
9. Monitoring.....	10
10. Sanctions prévues.....	10
11. Révision.....	11

CHARTRE D'UTILISATION DES RESSOURCES ET DISPOSITIFS INFORMATIQUES DES ÉLÈVES DE L'ÉCOLE EUROPÉENNE DE BRUXELLES IV (LAEKEN)

1. Préambule

Les Écoles européennes s'efforcent d'offrir aux élèves les meilleures conditions de travail en informatique et services multimédia. La présente Charte précise les règles de bon usage et bonne conduite des ressources informatiques à vocation pédagogique mises à leur disposition.

Cette Charte vient en annexe du Règlement intérieur de l'École européenne de Bruxelles IV (ci-après 'l'École') et s'inscrit dans le cadre des lois et règlements en vigueur, relatifs notamment au droit d'auteur, au droit de la propriété intellectuelle, à la protection de la vie privée (notamment du droit à l'image) et au traitement des données à caractère personnel ainsi qu'à la criminalité informatique.

2. Ressources et dispositifs informatiques

2.1. Définition

On entend par 'ressources et dispositifs informatiques' l'ensemble constitué par le réseau, les serveurs, les postes de travail de l'École, les tableaux interactifs, les périphériques (imprimantes, disques durs externes), les logiciels, les ordinateurs portables et tablettes, l'usage d'Internet à l'École et les ressources d'apprentissage numériques ¹fournis par cette dernière.

2.2. Règle d'or

L'utilisation des ressources informatiques de l'École européenne est uniquement réservé aux activités pédagogiques.

2.3. Access to IT resources and devices

L'accès aux ressources et dispositifs fournis par l'École est un privilège et non un droit. L'École se réserve le droit de révoquer ce privilège le cas échéant.

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

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

L'École peut procéder à des contrôles réguliers ou occasionnels pour vérifier que les ressources et dispositifs informatiques sont utilisés dans le respect des prescriptions de la présente Charte².

L'utilisation des ressources et dispositifs informatiques à l'École ou à distance, à la demande d'un enseignant, se fait sous la responsabilité de la Direction de l'École et sous le contrôle d'un membre de l'équipe éducative.

L'École propose l'accès à différentes ressources informatiques :

- Aux ordinateurs de l'école,
- Au réseau de l'École comprenant :
 - Des espaces de stockage des serveurs de l'école : espaces partagés ou limités à son compte personnel,
 - Des imprimantes réseaux,
- Aux services en ligne Office 365 (comprenant notamment un service de messagerie) gérés par l'École européenne,
- À des logiciels propriétaires sous licences ou libres,
- À Internet,
- À une connexion WiFi, en fonction des besoins éducatifs.

Tous les comptes d'accès fournis à l'élève sont personnels et ne peuvent être utilisés que par l'élève concerné. Ainsi, les codes d'accès doivent être absolument confidentiels et non divulgués à de tierces personnes (exception faite des représentants légaux de l'élève). Avant de quitter sa station de travail, l'élève doit toujours s'assurer qu'il s'est bien déconnecté.

L'élève préviendra son conseiller d'éducation en cas de problème avec son compte, en cas de perte, vol ou compromission de ses codes d'accès.

3. Règles générales de bonne conduite

3.1. Remarques générales

Le respect des règles générales de bonne conduite s'impose aux élèves lorsqu'ils utilisent les ressources et dispositifs mis à leur disposition par l'École à des fins pédagogiques. Ainsi, l'accès à ces ressources par l'élève qui utilise son appareil mobile personnel dans l'École (i.e., accès au réseau) ou à l'extérieur, implique également le respect de la présente Charte.

Pour un usage personnel à l'extérieur de l'école, chaque élève se voit offrir 5 licences d'installation d'Office 365 pour des ordinateurs et/ou des téléphones portables et tablettes.

² Les conditions de ce suivi sont définies à l'article 9 de la présente Charte ICT.

Ces licences ne peuvent être utilisées et installées que sur des dispositifs informatiques régulièrement utilisés par l'élève et protégés par un mot de passe dans le respect des règles générales de bonne conduites énoncées dans la présente Charte.

3.2. Respect de la confidentialité

Il est interdit à l'élève :

- De chercher à s'approprier le mot de passe d'autrui,
- De se connecter avec le nom d'utilisateur et mot de passe d'autrui,
- D'utiliser une session ouverte d'un autre utilisateur sans son autorisation explicite,
- D'ouvrir, de modifier ou d'effacer les fichiers d'autrui et de façon plus générale d'essayer d'accéder à des informations lui appartenant sans son autorisation,
- De faire une sauvegarde de mot de passe dans les logiciels d'internet comme Google chrome, Internet explorer, Firefox, etc., lors de l'utilisation de dispositifs non personnels.

3.3. Respect du réseau et des postes de travail

Les locaux et le matériel doivent être scrupuleusement respectés. Les claviers et les souris doivent être manipulés avec soin. Ainsi, les élèves ne sont pas autorisés à manger et boire lorsqu'ils utilisent les postes de travail au sein de l'École, afin de ne pas les endommager.

Il est interdit à l'élève :

- De chercher à modifier la configuration du poste de travail,
- De chercher à modifier ou de détruire des données du réseau ou du poste de travail,
- D'installer un logiciel ou de faire une copie d'un logiciel présent sur le réseau,
- D'accéder ou de tenter d'accéder à d'autres ressources que celles autorisées par l'École,
- D'ouvrir des messages, fichiers, documents, liens, images envoyés par des expéditeurs inconnus,
- D'introduire, dans quelque dispositif que ce soit, un lecteur amovible, sans l'autorisation d'un adulte responsable,
- De connecter un dispositif ou support de stockage (USB, GSM, autres) sans l'autorisation d'un adulte responsable,
- De perturber volontairement le fonctionnement du réseau, et notamment d'utiliser des programmes destinés à introduire des programmes nuisibles ou à contourner la sécurité (virus, logiciels espions ou autres),
- De détourner ou de tenter de détourner les systèmes de protection mis en place (pare feu, antivirus, etc.),

- D'utiliser des tunnels VPN³.

3.4. Respect des droits de propriété intellectuelle

Il est interdit à l'élève de :

- Télécharger ou effectuer des copies illégales de matériel (streaming, audio, films, logiciels, jeux, etc.) protégé par des droits de propriété intellectuelle,
- Plagier, c'est-à-dire reproduire, (re)diffuser, communiquer au public, sous quelque forme que ce soit, toute information, quel qu'en soit le support (tableau, graphique, équation, article de loi, image, texte, hypothèse, théorie, opinion, etc.), qui est protégée par un droit de propriété intellectuelle (droit d'auteur, etc.).

L'utilisation d'informations trouvées sur internet pour les travaux de classe implique que les sources soient comprises et correctement citées par l'élève. Ce dernier peut solliciter l'aide d'un des membres de l'équipe éducative à cet égard.

3.5. Respect des membres de la communauté scolaire et de l'École

Il est interdit à l'élève :

- D'afficher à l'écran, de publier des documents ou de prendre part à des échanges ayant un caractère diffamatoire, injurieux, extrémiste, pornographique, discriminatoire, que ce soit sur la base de l'origine raciale ou ethnique, des opinions politiques, de la religion ou des convictions philosophiques, ou de l'état de santé, ou de l'orientation sexuelle,
- D'harcéler autrui (cyber-harcèlement), en son nom ou à l'aide d'une fausse identité ou d'un pseudonyme (voir, à cet égard, la [politique anti-harcèlement de l'École](#)),
- D'utiliser les listes d'adresses électroniques ou données personnelles d'autrui à d'autres fins que celles visées par des objectifs pédagogiques ou éducatifs,
- D'utiliser un langage incorrect dans les emails, post, chats ou quelconque autre moyen de communication (l'auteur du message engage sa seule responsabilité sur le contenu expédié),
- De porter atteinte à la réputation d'un membre de la communauté scolaire ou de l'École, notamment par l'intermédiaire de diffusion de textes, d'images et/ou vidéos. Bien que l'école encourage le débat et favorise l'esprit critique, il est rappelé aux élèves que la liberté d'expression n'est pas absolue et qu'elle doit donc être exercée dans les limites fixées par les règlements pertinents et en tenant compte des droits et libertés d'autrui,

³ En informatique, un **réseau privé virtuel**, abrégé **VPN** – *Virtual Private Network*, est un système permettant de créer un lien direct entre des ordinateurs distants, en isolant ce trafic dans une sorte de tunnel.

- Contracter, vendre ou faire de la publicité, de quelque manière que ce soit, au nom de l'École, à moins d'avoir préalablement fait approuver son projet par la Direction de l'École.

4. Règles particulières pour l'usage d'Internet

4.1. Réseau de l'École

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

L'usage du réseau Internet pédagogique est réservé à des activités d'enseignement répondant aux missions des Écoles européennes.

Il est strictement interdit à l'élève :

- De se connecter à des services de dialogues en direct ou à des forums de discussion sauf autorisation contraire d'un membre de l'équipe éducative en raison de leur finalité pédagogique, ou à des réseaux sociaux,
- De partager des informations personnelles permettant l'identification de l'élève (prénom, noms, courrier électronique, adresse, etc.),
- D'accéder à des sites pornographiques, xénophobes, antisémites ou racistes vis-à-vis d'autres communautés,

Il est rappelé aux élèves que le racisme est une attitude d'hostilité ou de mépris systématique à l'égard de certains individus ou groupes de personnes sur base de leur nationalité, leur couleur de peau, leur ascendance, leur origine nationale ou ethnique⁴. Outre la race, la loi interdit également la discrimination fondée sur d'autres motifs tels que le sexe, les convictions politiques ou religieuses, l'orientation sexuelle, la langue et le handicap⁵,

- De télécharger et d'installer quelque programme que ce soit.

L'élève ne devra en aucun cas mentionner son nom, sa photo, son adresse, son numéro de téléphone ou tout autre information facilitant son identification sur Internet.

Il est interdit à l'élève d'utiliser l'adresse électronique liée à son compte O365 (...@student.eursec.eu) pour créer des comptes sur des applications, sites web ou software non autorisés par un membre de l'équipe éducative ou par la Direction de l'École.

4.2. Supervision et assistance de la session des élèves dans l'École

L'École utilise un système de supervision et d'assistance pour garder les élèves dans une dynamique d'apprentissage et pour permettre aux responsables du cours en question et

⁴ Article 4, 4°, de la loi du 10 mai 2007 modifiant la loi du 30 juillet 1981 tendant à réprimer certains actes inspirés par le racisme et la xénophobie.

⁵ Pour une liste complète des motifs de discrimination, veuillez-vous référer à la loi du 10 mai 2007 tendant à lutter contre certaines formes de discrimination.

aux responsables de la bibliothèque d'aider les élèves directement depuis leur poste de travail.

Seules les personnes autorisées par la Direction peuvent utiliser le logiciel de supervision et d'assistance, et sont tenues de respecter la Charte informatique applicable à leur rôle au sein de l'École.

Ce système permet :

- D'accéder aux écrans des élèves à distance, pour les aider et les garder concentrés sur leurs tâches,
- D'enseigner plus efficacement en diffusant l'écran du responsable du cours à la classe,
- De sélectionner les écrans des élèves pour présenter leur travail,
- De désactiver tous les écrans des élèves afin de capter leur attention.

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

4.3. Réseaux sociaux

Il est interdit à l'élève de se connecter aux réseaux sociaux avec l'adresse électronique liée à son compte O365 (...@student.eurasc.eu).

L'utilisation d'un dispositif numérique privé (téléphone, tablette, laptop) n'exonère pas l'élève du respect des règles de bon usage et de bonne conduite de la présente Charte, pour ce qui relève du respect des membres de la communauté scolaire et de l'École. L'élève demeure responsable du contenu diffusé. Le cyber-harcèlement fait l'objet de sanctions disciplinaires.

5. Règles particulières concernant l'apprentissage / l'enseignement en ligne

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

- Apprentissage ou enseignement en ligne à l'École ('blended learning'), impliquant l'utilisation de ressources d'apprentissage numérique approuvées par la Direction de l'École, ou la réalisation d'activités en ligne asynchrones (devoirs),
- Apprentissage ou enseignement en ligne à distance ('distance learning'), lors d'une suspension des cours dans l'École,
- Apprentissage ou enseignement en ligne à distance et in situ ('hybrid learning'), lorsque les cours sont suivis par une partie des élèves, in situ, et par une autre partie, à distance.

L'apprentissage ou l'enseignement en ligne implique l'utilisation volontaire de la caméra par l'enseignant ou l'élève. Il est obligatoire d'activer le son à la demande de l'enseignant, mais l'utilisation de la caméra est un choix personnel. Il est clair que la communication est plus

efficace si l'enseignant et l'élève peuvent se voir, mais le choix de l'utilisation de la caméra reste personnel.

En outre, il est interdit :

- De photographier et/ou filmer le(s) professeur(s) ainsi que les élèves participant à l'apprentissage en ligne à l'aide de dispositifs personnels, et a fortiori, de publier ces images/vidéos,
- De participer à des sessions d'apprentissage ou enseignement en ligne, à laquelle l'élève n'aurait pas été invité de manière expresse,
- D'inviter des participants aux sessions d'apprentissage ou enseignement en ligne, sans l'accord de la personne organisant la session,
- D'utiliser les ressources d'apprentissage numériques, pour intimider, harceler, diffamer ou menacer autrui.

Le droit à l'image est un droit reconnu pour chacun des membres de la communauté scolaire, c'est pourquoi l'École ne pourra tolérer l'utilisation d'images/vidéos prises à l'insu des personnes concernées.

6. Signalement à l'équipe éducative

L'élève s'engage à signaler à un membre de l'équipe éducative ou informatique (un conseiller, un coordinateur IT, un professeur, etc.), le plus rapidement possible :

- Tout logiciel ou dispositif suspect,
- Toute perte, vol ou compromission de ses informations d'authentification,
- Tout message, fichier, document, lien, image envoyé par un expéditeur inconnu.

Ce signalement doit être effectué en utilisant l'adresse électronique suivante : LIST-LAE-ICT@eursc.eu.

7. Protection des données

L'école s'engage à traiter les données personnelles collectées dans le cadre de l'utilisation des ressources informatiques dans le strict respect du Règlement général sur la protection des données et de la déclaration de confidentialité de l'école.

Toute question concernant le traitement des données personnelles des élèves dans le cadre de la présente Charte TIC peut être adressée au Délégué à la protection des données de l'école à l'adresse électronique suivante : LAE-DPO-CORRESPONDANT@eursc.eu.

8. Responsabilité

Les dommages intentionnels portés aux ressources informatiques de l'École peuvent entraîner des frais de réparation dans le chef des représentants légaux des élèves concernés, conformément à l'article 32 du Règlement général des Écoles européennes.

Tout élève qui choisit d'apporter un téléphone portable ou tout autre appareil électronique 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 dans le cas où les élèves sont tenus d'apporter un appareil à l'École pour les besoins du programme BYOD, cette dernière n'assumera aucune responsabilité pour la perte, le vol, les dommages ou le vandalisme d'un téléphone ou tout autre appareil, ou encore pour l'utilisation non autorisée d'un tel appareil.

9. Monitoring

L'administrateur informatique⁶ doit s'assurer constamment du bon fonctionnement et du bon usage des ressources informatiques. À cette fin, la surveillance du trafic réseau de l'école et des mac-adresses se connectant à l'Edu Wi-Fi ainsi que des appareils appartenant à l'école permet de détecter des anomalies (par exemple, une utilisation anormale du réseau, un espace de stockage excessif, une tentative de cyberattaque, un programme malveillant, etc.)

En cas d'anomalies détectées, l'administrateur informatique sollicite la Direction de l'École pour convenir des mesures à prendre. Cependant, en cas d'urgence absolue et pour protéger le système informatique de l'École, l'administrateur informatique peut prendre la décision immédiate de bloquer les accès informatiques à un ou plusieurs élèves, puis en référer immédiatement à la Direction.

Ce type d'intervention ne peut être effectué que moyennant le respect de finalités clairement définies, à savoir :

- La prévention de faits illicites ou diffamatoires, de faits 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 est attaché un caractère de confidentialité ;
- La sécurité et/ou le bon fonctionnement technique des systèmes informatiques, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'École ;
- Le respect en toute bonne foi des principes et règles d'utilisation des technologies disponibles, et de la présente Charte.

10. Sanctions prévues

L'élève qui contreviendrait aux règles énoncées ci-dessus s'expose aux sanctions disciplinaires prévues par le Règlement général des Écoles européennes et le Règlement interne de l'École, ainsi qu'aux sanctions et poursuites pénales prévues par la loi.

⁶ À l'école, chaque membre du département informatique est un « administrateur informatique ».

Le recours aux sanctions doit être raisonnable et proportionné aux circonstances du cas. À cet égard, la gravité de la faute de l'élève est évaluée sur la base de facteurs tels que l'âge de l'élève, l'intentionnalité, la répétition du manquement ou le manque de considération envers les membres de la communauté scolaire.

Tout membre de l'équipe éducative s'engage à faire respecter ces dispositions par les élèves qui sont sous sa responsabilité et se doit d'exercer un contrôle rigoureux.

11. Révision

Cette charte sera révisée à la lumière des expériences acquises au cours de l'année scolaire 2022/2023.