Collège

Amiral Pierre Bouvet

Charte régissant l'usage du système d'information par les personnels du collège Amiral Pierre Bouvet.

Région académique

Préambule

Le "système d'information" recouvre l'ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition par l'institution.
L'informatique nomade, tels que les assistants personnels, les ordinateurs portables, les téléphones portables…, est également un des éléments constitutifs du système d'information. Par « institution » il faut entendre tout service (administration centrale, rectorat, inspection académique), école, ou établissement d'enseignement scolaire. Le terme d'« utilisateur» recouvre tout personnel ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux ressources du système d'information quel que soit son statut.
Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires, notamment le respect des règles visant à assurer la sécurité, la performance des traitements et la conservation des données. **La présente charte définit les règles d'usages et de sécurité que l'institution et l'utilisateur s'engagent à respecter : elle précise les droits et devoirs de chacun.**

Engagements de l'institution :
L'institution porte à la connaissance de l'utilisateur la présente charte. Elle met en œuvre les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisateurs. L'institution facilite l'accès des utilisateurs aux ressources du système d'information. Les ressources mises à leur disposition sont prioritairement à usage professionnel mais l'institution est tenue de respecter l'utilisation résiduelle du système d'information à titre privé.

Engagements de l'utilisateur :
L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès. Il a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie. En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat.

Article I. Champ d'application

Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent à l'institution ainsi qu'à l'ensemble des utilisateurs.

Article II. Conditions d'utilisation des systèmes d'information

Section 2.01 Utilisation professionnelle / privée

Les systèmes d'information (notamment messagerie, internet ...) sont des outils de travail ouverts à des usages professionnels administratifs et pédagogiques. L'utilisateur est responsable de son espace de données à caractère privé. Lors de son départ définitif de l'établissement, il lui appartient de récupérer son espace de données à caractère privé, la responsabilité de l'administration ne pouvant être engagée quant à la conservation de cet espace. Les mesures de conservation des données professionnelles sont définies avec le responsable désigné au sein de l'institution. L'utilisation des systèmes d'information à titre privé doit rester exceptionnelle et respecter la réglementation en vigueur.

Article III. Principes de sécurité

Section 3.01 Règles de sécurité applicables

L'institution met en œuvre les mécanismes de protection appropriés sur les systèmes d'information mis à la disposition des utilisateurs. Les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est conférée. La sécurité des systèmes d'information mis à sa disposition lui impose :
- de respecter les consignes de sécurité, notamment les règles relatives à la gestion des codes d'accès ;
- de garder strictement confidentiels son (ou ses) codes d'accès et ne pas le(s) dévoiler à un tiers ;
- de respecter la gestion des accès, en particulier ne pas utiliser les codes d'accès d'un autre utilisateur, ni chercher à les connaître.

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisateur nécessite plusieurs précautions:

1) de la part de l'institution :
-veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées, en dehors des mesures d'organisation de la continuité du service mises en place par la hiérarchie ;
-limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité ;

2) de la part de l'utilisateur :
-s'interdire d'accéder ou de tenter d'accéder à des ressources du système d'information, pour lesquelles il n'a pas reçu d'habilitation explicite ;
-ne pas connecter directement aux réseaux locaux (filaire et/ou wifi) des matériels autres que ceux confiés ou autorisés par l'institution dans le cadre de cette charte ;
-ne pas installer, télécharger ou utiliser sur le matériel de l'institution, des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, ou sans autorisation de sa hiérarchie ;
-se conformer aux dispositifs mis en place par l'institution pour lutter contre les virus et les attaques par programmes informatiques ;

Section 3.02 Devoirs de signalement et d'information
L'utilisateur doit avertir sa hiérarchie sans délai de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le système d'information, etc. Il signale également à la personne responsable du site toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation.

Section 3.03 Mesures de contrôle de la sécurité
L'utilisateur est informé :
- que pour effectuer la maintenance corrective, curative ou évolutive, l'institution se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition
- qu'une maintenance à distance est précédée d'une information de l'utilisateur ;
- que toute information bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire, sera isolée ; le cas échéant supprimée.
L'institution informe l'utilisateur que le système d'information donne lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable.
Les personnels chargés des opérations de contrôle des systèmes d'information sont soumis au secret professionnel. Ils ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions dès lors que ces informations sont couvertes par le secret des correspondances ou identifiées comme telles, elles relèvent de la vie privée de l'utilisateur. En revanche, ils doivent communiquer ces informations si elles mettent en cause le bon fonctionnement technique des applications ou leur sécurité.

Section 3.04 Utilisation de matériel personnel sur l'infrastructure de l'institution
Les personnels amenés à utiliser leur équipement personnel dans un but professionnel sur les infrastructures de l'institution doivent bénéficier de l'accord de leur hiérarchie et s'assurer du bon niveau de sécurité de leur équipement (antivirus en fonctionnement et à jour, un système d'exploitation à jour) afin de ne pas perturber le fonctionnement de l'établissement. Pour cela, l'institution met à disposition des personnels académiques l'antivirus Trend-Micro récupérables à https://edu.trendmicro.fr/ .

Article IV. Communication électronique

Section 4.01 Messagerie électronique
L'institution s'engage à mettre à la disposition de l'utilisateur une boîte à lettres professionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques. L'aspect nominatif de l'adresse électronique constitue le simple prolongement de l'adresse administrative : il ne retire en rien le caractère professionnel de la messagerie. L'adresse électronique nominative est attribuée à un utilisateur qui la gère sous sa responsabilité.

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles[11] 1369-1 à 1369-11 du code civil. L'utilisateur doit, en conséquence, être vigilant sur la nature des messages électroniques qu'il échange au même titre que

pour les courriers traditionnels. Chaque utilisateur doit organiser et mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve.
Chaque utilisateur veillera à l'entretien de sa messagerie professionnelle, notamment à ne pas dépasser le quota de stockage qui lui est attribué qui pourrait perturber la bonne réception des messages professionnels.

Section 4.02 Internet

Il est rappelé qu'Internet est soumis à l'ensemble des règles de droit en vigueur. L'utilisation d'Internet (par extension intranet) constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'accessibilité de l'information au sein et en dehors de l'institution. Internet est un outil de travail ouvert à des usages professionnels (administratifs et pédagogiques). Si une utilisation résiduelle privée peut être tolérée, il est rappelé que les connexions établies grâce à l'outil informatique mis à disposition par l'administration sont présumées avoir un caractère professionnel.

(a) Publication sur les sites internet et intranet de l'institution : toute publication de pages d'information sur les sites internet ou intranet de l'institution doit être validée par un responsable de site ou responsable de publication nommément désigné.

(b) Sécurité : L'Institution se réserve le droit de filtrer ou d'interdire l'accès à certains sites. Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'institution. L'utilisateur est informé des risques et limites inhérents à l'utilisation d'Internet par le biais d'actions de formations ou de campagnes de sensibilisation.

Section 4.03 Téléchargements

Tout téléchargement de fichiers, notamment de sons ou d'images, sur Internet doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis à l'article VI. L'institution se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information.

Article V. Respect de la propriété intellectuelle

Chaque utilisateur doit :
- utiliser les logiciels dans les conditions des licences souscrites ;
- ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

Article VI. Respect de la loi informatique et libertés

L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel, conformément à la loi n° 78-17 du 6 janvier 1978 dite « Informatique et Libertés » modifiée, par la loi n° 2004-801 du 6 août 2004 et la loi RGPD du 25 mai 2018.

Article VII. Limitation des usages

En cas de non-respect des règles définies dans la présente charte et des modalités définies dans les guides d'utilisation établis par le service ou l'établissement, la « personne juridiquement responsable » pourra, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des personnels, limiter les usages par mesure conservatoire. Par « personne juridiquement responsable », il faut entendre toute personne ayant la capacité de représenter l'institution (ministre, directeur, recteur, inspecteur d'académie, chef d'établissement...).

Article VIII. Entrée en vigueur de la charte

La présente charte à valeur de règlement intérieur pour ce qui concerne l'usage des systèmes d'information. Elle fait également l'objet d'une communication devant le conseil d'administration des établissements. **Le présent document prévaut sur tout autre document (ou charte) relatif à l'utilisation des systèmes d'information.**

Nom et prénom : **Date :** **Signature :**