Charte du Bon usage de l'Informatique et des réseaux pédagogiques

Domaine d'application

Ces règles s'appliquent à tout utilisateur des réseaux pédagogiques au sein de l'établissement.

On appelle utilisateur toute personne, quel que soit son statut : élève, enseignant, technicien, administratif, stagiaire…, appelée à utiliser les ressources informatiques et réseaux pédagogiques de l'établissement.

Tout utilisateur, lors de la cessation de son activité au sein de l'établissement, garde son habilitation à utiliser les moyens et ressources informatiques de l'ensemble lycées-collège-enseignement supérieur pendant un an.

L'utilisation des IPAD confiés aux élèves et professeurs à leur arrivée, est gérée par la convention de mise à disposition.

Accès au réseau (filaire et wifi)

Il y a lieu de considérer que toute personne travaillant ou étudiant dans l'établissement est utilisateur potentiel des moyens ou ressources informatiques de l'établissement.

Tout utilisateur de ces moyens et ressources informatiques a le devoir de respecter les règles de l'établissement. La sécurité du réseau informatique passe par le respect de ces règles et la vigilance de chacun. Face aux risques, une pédagogie permanente s'impose, elle concerne tout responsable et tout personnel.

L'accès au réseau pédagogique se fait sous la responsabilité du chef d'établissement. Notre établissement est lui- même soumis aux règles de bonne utilisation des moyens informatiques et se doit de faire respecter les règles déontologiques en vigueur et la loi.

L'usage de ce réseau pédagogique se fait dans le respect des projets éducatif, d'établissement, du règlement intérieur et de la charte du Bon usage de l'Informatique et des réseaux. Le non-respect du règlement intérieur ou/et de la Charte du Bon usage de l'Informatique et des réseaux pédagogiques engage la responsabilité de l'utilisateur.

« Nul n'est censé ignorer la loi »

1. Conditions d'accès aux ressources informatiques

☑ L'utilisation des moyens informatiques pédagogiques de l'établissement a pour objet exclusif de mener des activités pédagogiques, d'enseignement ou de recherche ou d'effectuer des recherches d'informations à but scolaire ou professionnel. Sauf autorisation préalable du Chef d'établissement, ces moyens ne peuvent être utilisés à d'autres fins. (Toutes les utilisations à fin lucrative sont interdites.)

☑ Chaque utilisateur se voit attribuer un compte individuel (nom d'utilisateur, mot de passe) qui lui permettra de se connecter au réseau pédagogique, un historique de connexion sera conservé conformément à la loi.

☑ Le mot de passe est personnel et provisoire. Chaque utilisateur est tenu de le modifier par un mot de passe personnel. L'utilisateur préviendra l'administrateur s'il soupçonne la violation de son compte.

☑ Tout compte Office365 suspecté d'être utilisé de façon illicite pourra être bloqué par le Conseil de Direction de l'établissement. L'élève concerné sera alors convoqué afin d'identifier les manquements face à la Charte Informatique. Le compte pourra ensuite être réinitialisé avec la création d'un nouveau mot de passe pour éviter toute fraude.

2. Missions et devoirs des administrateurs

L'ensemble des ordinateurs, tablettes et réseaux pédagogiques est géré par un ou plusieurs administrateurs.

Les administrateurs :
☑ gèrent le compte des utilisateurs et les informent sur les droits attribués à chacun,
☑ mettent leurs compétences au service du bon fonctionnement des moyens de l'établissement
☑ informent les utilisateurs de toute intervention susceptible de perturber ou interrompre l'utilisation habituelle des moyens informatiques,
☑ sensibilisent les utilisateurs aux problèmes de sécurité informatique relatifs au système, font connaître les règles de sécurité à respecter,
☑ respectent les règles de confidentialité des informations (« secret professionnel », « discrétion professionnelle »),
☑ respectent, en tant qu'utilisateur du système, les règles qu'ils sont amenés à imposer aux autres, informent le Chef d'établissement de toute anomalie ou manquement à la charte constaté
…,
☑ peuvent contribuer, sur demande du Chef d'établissement, à la mise en place d'un système de filtrage d'accès Internet.

3. Respect de la déontologie informatique

Chaque utilisateur s'engage à respecter les règles de déontologie informatique énoncées ci-dessous.

➢ Principes de base

L'utilisateur ne doit pas :
☑ masquer sa véritable identité sur le réseau local,
☑ usurper l'identité d'autrui ou s'approprier le mot de passe d'un autre utilisateur,
☑ introduire, modifier, altérer, falsifier, copier ou supprimer des informations ne lui appartenant pas,
☑ accéder à des informations appartenant à un autre utilisateur sans son autorisation,
effectuer des activités accaparant les ressources informatiques et pénalisant la communauté (impression de gros documents, stockage de gros fichiers, encombrement de la boîte aux lettres électronique…)
☑ se livrer à des actes de piratage.
☑ stocker des fichiers d'origine illégale (ceux-ci seront détruits par le service informatique sous couvert du Chef d'Etablissement).
☑ masquer son adresse IP.

L'utilisateur doit :
☑ respecter les règles :
- d'accès aux ressources informatiques,
- d'usage des matériels informatiques, notamment les procédures de connexion et déconnexion préconisées,
☑ prendre soin du matériel et des locaux mis à disposition,
☑ appliquer les règles de sécurité préconisées,
☑ informer les administrateurs de toute anomalie constatée,
☑ fournir l'adresse MAC de tout appareil personnel afin de pouvoir se connecter au réseau wifi (non possible pour les élèves et étudiants).

➢ Respect de l'intégrité du système informatique

L'utilisateur ne doit pas :
☑ effectuer des opérations pouvant nuire au fonctionnement normal du réseau,
☑ mettre en place un dispositif pour contourner la sécurité,
☑ installer ou utiliser un logiciel sans autorisation,
☑ introduire ou modifier frauduleusement des données,
☑ modifier la configuration du système sans autorisation,
☑ débrancher le matériel et systèmes installés dans les salles de classe.

➢ Usage des services Internet (Web, messagerie, forum…)

L'utilisateur ne doit pas :

☑ harceler ou porter atteinte à l'intégrité ou à la dignité humaine d'un autre utilisateur, notamment par l'intermédiaire de messages, textes ou images provocants,

L'utilisateur ne doit pas :

☑ diffuser des informations :

- injurieuses ou diffamatoires
- pouvant porter atteinte à la vie privée ou aux droits et à l'image d'autrui,
- faisant l'apologie du racisme, de la pornographie, de la pédophilie, de la xénophobie et de l'homophobie, de l'usage de produits illicites, etc.
- pouvant porter atteinte à l'ordre public,
- faisant la promotion, sans autorisation d'un membre de l'équipe de direction, d'activité de sites Internet, réseaux sociaux, n'ayant aucun lien avec les activités d'enseignement de l'établissement

☑ consulter des sites à caractère immoral, xénophobe, raciste, pédophile ou pornographique, terroriste,

☑ utiliser les groupes de discussion « chat » et « forums » ou télécharger des logiciels ou documents sans autorisation préalable sauf dans le cadre d'une activité pédagogique ou professionnelle.

Chaque membre de l'établissement ayant à disposition une tablette et/ou ayant un compte OFFICE 365 associé à l'établissement est responsable du contenu et de l'utilisation de toutes les applications (messagerie, drive, réseaux sociaux, etc…)

La tablette et/ou l'accès aux ressources informatiques ou au compte OFFICE 365 pourront lui être retirés en cas de non-respect de la charte.

4. Protection des personnes

➢ Respect du droit de propriété intellectuelle

L'utilisateur et les administrateurs ne doivent pas :

☑ faire des copies de logiciels commerciaux non autorisées par la loi (seules les copies de sauvegarde sont autorisées),

☑ installer ou utiliser des copies illégales,

☑ contourner les restrictions d'utilisation d'un logiciel.

➢ Protection des libertés individuelles

La création de tout fichier contenant des informations nominatives doit faire l'objet d'une autorisation préalable du Chef d'établissement de façon à respecter la procédure réglementaire (demande auprès de la Commission Nationale de l'Informatique et des Libertés). La divulgation ou le détournement des informations collectées sont interdits.

Les personnes concernées doivent être informées préalablement de la constitution du fichier.

➢ Respect du secret de la correspondance

L'utilisateur et les administrateurs doivent :

☑ strictement respecter le secret de la correspondance privée.

5. Publication sur le site Internet de l'établissement

Toute publication sur le site Internet, les réseaux sociaux de l'établissement, ou autre, se fait sous le contrôle et la responsabilité du Chef d'établissement.

Il convient de respecter la réglementation concernant la propriété intellectuelle, les droits d'auteur et des principes de la République et les valeurs du projet d'établissement.

Les règles suivantes s'imposent à tous pour une publication sur le site Internet :

- Les ressources doivent être originales et ne doivent pas être assujetties à des droits d'auteurs.
- Les informations diffusées ne doivent pas être erronées.
- La source des documents est clairement indiquée.
- Aucune publicité commerciale ne doit figurer.
- Le droit à l'image doit être respecté.

Toute publication doit respecter le projet éducatif de l'établissement.

6. Contrôle et sanctions

Les demandes envoyées au réseau par les utilisateurs sont stockées dans un fichier Log. Ce fichier peut être communiqué aux autorités judiciaires sur commission rogatoire.
Le Chef d'établissement se réserve la possibilité d'examiner le contenu de ces fichiers, de façon ponctuelle et exceptionnelle, notamment en cas de violation soupçonnée des principes de cette charte (à l'exception du contenu des courriers électroniques afin de respecter la loi sur la confidentialité de la correspondance).
Le Chef d'établissement a pleine autorité pour prendre les mesures conservatoires nécessaires en cas de manquement à la présente charte et notamment l'interdiction de l'utilisation des moyens informatiques et réseaux ainsi que la confiscation temporaire dont la durée sera laissée à l'appréciation du chef d'établissement, des téléphones portables ou tout autre objet connecté.

Le non-respect des règles et obligations définies dans la présente charte ainsi que le non-signalement des tentatives de violation de son compte sont passibles de sanctions de nature :

☑ disciplinaire : les utilisateurs fautifs sont passibles de sanctions disciplinaires et par conséquent, peuvent être déférés devant les instances compétentes.
☑ civile : des condamnations civiles prévues par les textes législatifs et réglementaires en vigueur peuvent être encourues.
☑ pénale : des condamnations pénales sont prévues par les textes législatifs et réglementaires.

7. Le Règlement Général sur la Protection des Données de l'Union européenne

L'établissement respecte le RGPD de l'Union européenne. Pour cela :

- Le service informatique tient à jour le registre des activités de traitement des données.
- La gouvernance interne pour le respect du RGPD est assurée par la commission informatique présidé par le Directeur Adjoint qui se réunit une fois par semaine ouvrée,
- Le service informatique, sous couvert du directeur adjoint délégué à la protection des données, notifiera tout incident aux autorités dans un délai de 72 heures.
- Afin de sécuriser le stockage des données, l'usage des clefs USB et disques durs externes sont interdits

8. Textes législatifs et réglementaires

Loi « informatique et liberté » n° 78-17 du 06 janvier 1978
Loi sur l'accès aux documents administratifs n° 78-753 du 17 juillet 1978
Loi « liberté de la presse » du 29 juillet 1981
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 10 juillet 1989
Loi sur le code de la propriété intellectuelle du 1er juillet 1992
Sanctions pénales ~ Extrait de la loi du 5 janvier 1986, relative à la fraude informatique, dite Loi Godfrain :

- Article 462-2 *: Quiconque, frauduleusement aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé des données, sera puni d'un emprisonnement de deux mois à un an et d'une amende de 2000 francs à 50000 francs ou de l'une de ces deux peines seulement. Lorsqu'il en sera résulté soit par la suppression ou la modification des données contenues dans le système, soit par altération du fonctionnement de ce système, l'emprisonnement sera de deux mois à deux ans et l'amende de 10000 francs à 100000 francs.*
- Article 462-7 *: La tentative des délits prévus par les articles 462-2 à 462-6 est punie des mêmes peines que le délit lui-même…*

LOI n° 2018-698 du 3 août 2018 relative à l'encadrement de l'utilisation du téléphone portable dans les établissements https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=9AC71E97CDCECA793045F11D40DD791D.tplgfr23s_2?cidTexte=JORFTEXT000037284333&idArticle=LEGIARTI000037285417&dateTexte=20180806
LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.