# CHARTE D'UTILISATION DES RESSOURCES INFORMATIQUES

Actuellement, il est difficile de concevoir le traitement de l'information de manière isolée. Les différents moyens de traitement sont en grande partie reliés entre eux, que ce soit sur place par des réseaux locaux ou à l'extérieur au moyen de plus grands réseaux fédérateurs (notamment le réseau Internet).

Cette interconnexion permet à chacun d'accéder à un ensemble important de ressources informatiques, donnant ainsi la possibilité de mettre en commun les connaissances les plus variées. En contrepartie, il est difficile de préserver la confidentialité ainsi que la défense du domaine privé. Il est donc nécessaire de respecter un certain nombre de règles de base pour assurer la liberté et la protection de chacun dans l'utilisation des moyens informatiques. La formation et la sensibilisation des utilisateurs des TICE dans les établissements d'enseignement doivent se concrétiser par la responsabilisation des apprenants et des personnels.

## OBJECTIFS

La présente charte a pour objet :

1. d'informer les utilisateurs des moyens informatiques de l'EPLEFPA du Bourbonnais au sujet :
   - des règles de bon usage des moyens informatiques ;
   - des principes déontologiques qui s'imposent à tous en la matière ;
   - des dispositions législatives et réglementaires qui régissent ce domaine d'activité et des sanctions encourues en cas d'infraction ;
2. de recueillir leur engagement à respecter ces règles afin de leur donner l'autorisation et la marche à suivre pour se connecter au réseau de l'établissement.

Ces règles à respecter relèvent avant tout du bon sens et ont pour but d'assurer à chacun une utilisation optimale des ressources informatiques de l'établissement, compte tenu des contraintes globales imposées par leur partage et de la difficulté de maintenir un tel réseau.

## DOMAINE D'APPLICATION

Les règles et obligations énoncées ci-dessous s'appliquent à chaque utilisateur des ressources informatiques dans les locaux de l'établissement.

On appelle **utilisateur** toute personne appelée à utiliser les moyens informatiques de l'établissement, quel que soit son statut : élève majeur ou mineur, étudiant, enseignant, formateur, technicien, agent administratif, personnel de direction, stagiaire, invité…

Les **ressources informatiques** sont constituées des **équipements** (postes de travail, serveurs, imprimantes, scanners, commutateurs réseau, modems, tableaux interactifs, etc), de leurs **connections** (câbles réseaux en cuivre, alimentations secteurs, fibres optiques, réseaux sans-fil, etc), des **logiciels** et des **données numériques**, et des **services** fournis par ces systèmes (accès Internet, courriel, partage de fichiers, impression de documents, etc)

Les **locaux** concernés comprennent d'abord les salles informatiques de cours ou en accès libre, le CDR, tout local contenant une ressource telle que définie plus haut, mais aussi toutes les zones couvertes par le (futur) réseau sans-fil. De plus, les règles définies par la présente charte s'étendent également à toute utilisation, à partir du réseau local, de ressources informatiques externes accessibles par Internet aussi bien qu'à un accès externe par Internet au système local des Espaces Numériques de Travail par exemple.

## CONDITIONS D'ACCES

L'utilisation des ressources informatiques de l'établissement est soumise à une autorisation préalable ; celle-ci est concrétisée par **l'ouverture d'un compte et l'acceptation des règles d'utilisation de ces ressources**.

Ce **compte d'accès** est composé d'un **identifiant** et d'un **mot de passe**. Pour les ordinateurs portables nomades, il comprend en plus 3 adresses IP, un masque de sous réseau, et si nécessaire une clé de cryptage des données WiFi.

**Il est délivré à titre personnel, incessible et temporaire. Il ne doit pas être communiqué à quelqu'un d'autre. Son vol ou sa perte doivent être signalés rapidement aux administrateurs du système.**

Le droit d'accès est limité à des activités conformes aux missions de l'établissement. Par ailleurs, l 'étendue des ressources informatiques auxquelles l'utilisateur a accès peut être limitée en fonction de ses besoins réels et des contraintes imposées par le partage de ces ressources avec les autres utilisateurs.

Le droit d'accès est retiré dès lors que le statut de l'utilisateur ne le justifie plus. Il peut également être retiré, par mesure conservatoire, par les administrateurs réseau de l'établissement, si le comportement de l'utilisateur n'est plus compatible avec les règles énoncées dans la présente charte.

**Le non-respect des règles énoncées dans le présent document engage la responsabilité personnelle de l'utilisateur car il est tenu pour responsable de toute utilisation des ressources informatiques faites à partir de son compte.**

## REGLES D'UTILISATION

De manière générale, l'utilisation des ressources informatiques de l'établissement est soumise au respect des règles essentielles de la vie en communauté, du bon sens et des règles de correction minimales.

1. Il doit être fait un usage raisonnable de toutes les ressources informatiques partagées afin de maintenir une qualité de service des équipements (espace disque, durée d'occupation des postes de travail) suffisante pour tous les utilisateurs.
2. L'utilisateur est responsable de l'emploi des ressources informatiques dont il a l'usage. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale et de signaler au service informatique toute anomalie qu'il constate dans le fonctionnement du réseau ou des ressources.
3. L'utilisateur doit respecter la législation en vigueur (voir annexe 1)

**Plus particulièrement l'utilisateur ne doit en aucun cas :**

- masquer son identité lors de l'accès aux ressources ;
- obtenir le mot de passe d'un autre utilisateur par vol, utilisation de logiciels espions ou tout autre moyen de craquage des mots de passe utilisateurs ou système ;
- altérer des données ou accéder à des informations appartenant à d'autres utilisateurs, sans leur autorisation explicite ;
- porter atteinte à l'intégrité d'un autre utilisateur, à sa personnalité ou à sa sensibilité par un quelconque moyen informatique (par l'intermédiaire de messages, de textes, de sons, d'images fixes ou animées, etc...) ;
- effectuer des copies de logiciels, de CD ou de DVD : qu'ils soient physiquement dans l'établissement ne signifie pas qu'ils sont libres de droits, l'autorisation de copie doit être accordée spécifiquement par les administrateurs du système ;
- télécharger des logiciels, des musiques, des images, des films, qui ne sont pas libres de droits ou pour des motifs non pédagogiques (fichiers de jeux, mp3, Divx, etc...) ;
- perturber le fonctionnement normal du réseau ou des systèmes qui y sont connectés par manipulation anormale, introduction de données ou de logiciels nuisibles (virus, vers, bombes et chevaux de Troie), par saturation des services du réseau ou par contournement des systèmes de sécurité ;
- accéder, modifier ou supprimer des matériels ou des données ne lui appartenant pas sur les systèmes et notamment : modifier la configuration des machines, installer ou supprimer tout logiciel fourni sur support amovible ou téléchargé par le réseau local ou externe, modifier les connections réseau internes ou externes du système que ce soit au niveau matériel ou logiciel ;
- cracker ou hacker des machines de l'établissement ou externes, des logiciels, ou des réseaux ;
- manger ou boire sur un poste de travail (imprimantes et scanners compris) ;

- inciter un autre utilisateur à ne pas respecter ces règles.

**L'utilisation d'Internet** doit être dédiée prioritairement à des activités pédagogiques ou administratives correspondant aux missions de l'Enseignement Agricole. Il est donc interdit de naviguer sur des sites violant les lois françaises (cf annexe 1) ou de nature à heurter la sensibilité admise couramment dans un établissement public d'enseignement agricole. C'est à dire, de manière non exhaustive : faisant étalage de pornographie, promotion de drogues illégales, incitation à des activités illégales, au racisme, à l'anti-sémitisme, à la violence, de prosélytisme sectaire, d'opinions révisionnistes ou négationnistes, de jeux d'argent en ligne, etc.

Pour faire respecter ces consignes, une surveillance des séances de navigation Internet par un adulte sera la règle : enseignant dans les salles de cours, documentaliste au CDR, personnel de vie scolaire en salle libre accès et à l'internat – dans la mesure du possible. Des dérogations seront possibles dans le cas des apprenants majeurs en accès libre.

Lors de l'utilisation des outils de communication électroniques (courriel, chat, forums de discussion et blogs) les règles suivantes devront être respectées :

- respect de la netiquette : correction des propos – politesse de base
- dans des communications à diffusion publique (blogs, forums, chat) on devra préciser si on s'exprime à titre personnel ou bien au nom de l'établissement
- le contenu des propos et des pièces jointes (fichiers attachés) devra respecter les lois en vigueur (cf annexe 1) et plus particulièrement ne pas diffamer, calomnier ou diffuser une image non autorisée d'autrui ou de l'établissement

## MOYENS DE CONTROLE

L'utilisateur accepte que l'établissement, pour faire respecter cette charte, prenne des mesures adéquates pour stopper les utilisations non autorisées des services ou les perturbations du fonctionnement quelles provoquent : identifier l'utilisateur responsable et le caractère accidentel ou volontaire de son action, stopper l'action nuisible et corriger les dégâts, sanctionner l'utilisateur si nécessaire pour assurer réparation du dommage et éviter la répétition du problème.

Il accepte donc que les responsables du système informatique mettent en place et utilisent tout dispositif permettant :

- d'identifier les auteurs des perturbations (traces informatiques, fichiers logs, webcams, historiques de sites webs consultés, logiciels de contrôles à distance des postes de travail, etc)
- d'optimiser l'utilisation des ressources (espaces disques durs, volumes des accès réseaux, etc...)
- et de recueillir et de conserver des données utilisateurs nécessaires à la bonne marche du système.

Ces contrôles ne pourront porter sur le contenu même des fichiers personnels mais sur leur nombre, leur taille cumulée, leur emplacement de stockage, leur fréquence d'utilisation, leur origine et leur type de fichier (texte, logiciels ou données, sons mp4, mp3, vidéos divx ou avi, etc...) – et l'espace privatif de l'utilisateur sera respecté. En aucun cas les données obtenues ne serviront à un contrôle individuel illégal.

De plus, dans le cadre des séances pédagogiques utilisant les outils numériques, en salle informatique et au CDR (Centre de Ressources et de Documentation), un dispositif de surveillance des écrans des ordinateurs et de prise de contrôle à distance est mise à la disposition des enseignants.

## SANCTIONS APPLICABLES

Les lois et textes réglementaires définissent les droits et obligations des utilisateurs de ressources informatiques que ce soit à domicile ou dans le cadre public de l'établissement. Elles sont rappelées et synthétisées dans l'annexe 1 de ce document et sont censées être connues de chaque utilisateur. Il est donc tout à fait possible que des **sanctions pénales** soient demandées, en cas d'infraction constatée à ces lois, dans le cadre de poursuites judiciaires.

De plus, et de manière indépendante, des sanctions administratives internes à l'établissement peuvent être appliquées en cas de non respect des règles d'utilisation définies dans cette charte. Elles peuvent agir à deux niveaux :

- au niveau des **mesures conservatoires** (pour assurer la sécurité du système), ces sanctions peuvent englober l'interdiction d'utiliser l'outil informatique seul (en dehors des cours), l'interdiction totale d'accès au système (par inactivation temporaire ou définitive du compte utilisateur), sans préjuger d'une obligation éventuelle de réparation du dommage ;
- au niveau des **dispositions réglementaires générales** : avertissement, conseil de discipline, exclusion de l'établissement pourront également être requis selon la gravité du dommage.

## LE DROIT D'ACCES DE L'UTILISATEUR A SES DONNEES A CARACTERE PERSONNEL : RGPD

Suite à la parution de règlement (UE) n°2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD) et à la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, l'utilisateur dispose de droits sur le traitement de ses données personnelles sur supports informatiques. Il peut les faire valoir auprès du directeur de l'établissement en tant que responsable des traitements pour l'établissement. Ces droits sont détenus par l'utilisateur s'il a au moins 15 ans ou par ses représentants légaux s'il a moins de 15 ans.

Il s'agit notamment du :

• droit d'accès aux données (article 15 RGPD)

• droit de rectification (article 16 RGPD) : L'utilisateur a le droit de demander que ses données soient rectifiées ou complétées, et ce dans les meilleurs délais.

• droit d'effacement ou « droit à l'oubli » (article 17 RGPD) : L'utilisateur a le droit de demander l'effacement de ses données, dans les meilleurs délais si le traitement n'entre pas dans le champ de la mission de service public de l'éducation.

• droit à la portabilité des données (article 20 RGPD) : L'utilisateur a le droit de récupérer les données qu'il a fournies à l'établissement, dans un format structuré, couramment utilisé et lisible par machine, et de les transmettre à un autre établissement ou organisme.

• droit d'opposition (article 21 RGPD) : L'utilisateur a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel. Ce droit s'exprime dans la limite des obligations légales fixées aux établissements par l'administration.

## ANNEXE 1 *Cadre législatif*

**1. Informatique et libertés** (loi du 6 janvier 1978) qui porte notamment création de la Commission Nationale Informatique et Libertés (CNIL), complétée par la loi du 22 juillet 1992 qui protège tout individu contre tout usage abusif, ou malveillant, d'informations le concernant et figurant dans un fichier informatique quelconque. Elle prévoit, en particulier,

- que la création de tout fichier contenant des informations nominatives doit faire l'objet de formalités préalables à sa mise en oeuvre auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

- que toute personne sur laquelle des informations figurent dans un tel fichier doit être informée de l'existence de ce fichier, de sa finalité, de l'existence d'un droit d'accès et des modalités de mise en oeuvre de celui-ci, dès la collecte des informations le concernant.

- que toute personne figurant dans un tel fichier informatique a le droit de faire rectifier ses données personnelles à tout moment.

**2. Protection des logiciels** (loi n° 85.660 du 3 juillet 1985) intégrée au Code de la **propriété intellectuelle** (loi n° 92.597 du 1er juillet 1992) et des **bases de données** (articles L341-1 et suivants du Code de la propriété intellectuelle) interdisant à l'utilisateur de reproduire tout ou partie de logiciels ou de données non libres de droits d'utilisation ou d'exploitation commerciale.

**3. Protection du droit d'auteur, des marques, des dessins et modèles** (Livres I, V, et VII du Code de la propriété intellectuelle)

**4. Loi sur la fraude informatique** du 5 janvier 1988 qui complète le titre II du livre III du Code Pénal par un troisième chapitre ainsi rédigé : **Chapitre III - De certaines infractions en matière informatique**

***Article 462-2***. - Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données sera puni d'un emprisonnement de deux mois à un an et d'une amende de 305 € à 7 622,50 € ou de l'une de ces deux peines. Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit d'une altération du fonctionnement de ce système, l'emprisonnement sera de deux mois à deux ans et l'amende de 1 524,50 € à 15 245 €.

***Article 462-3***. - Quiconque aura, intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1 524,50 € à 15 245 €. ou de l'une de ces deux peines.

***Article 462-4***. - Quiconque aura, intentionnellement et au mépris des droits d'autrui, introduit des données dans un système de traitement automatique ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 305 € à 76 224 € ou de l'une de ces deux peines.

***Article 462-5***. - Quiconque aura procédé à la falsification de documents informatisés, quelle que soit leur forme, de nature à causer préjudice à autrui, sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 3 049 € à 30 490 € ou de l'une de ces deux peines.

***Article 462-6***. - Quiconque aura sciemment fait usage des documents informatisés visés à l'article 462-5 sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 3 049 € à 30 490 € ou de l'une de ces deux peines.

***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.

***Article 462-8***. - Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues par les articles 462-2 à 462-6 sera puni pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

***Article 462-9***. - Le tribunal pourra prononcer la confiscation des matériels appartenant au condamné et ayant servi à commettre les infractions prévues au précédent chapitre.

**Voir aussi les articles 323-1 et suivants du Code Pénal**

**5. Confidentialité et protection des données personnelles** (loi n° 78.17 du 6 janvier 1978, modifiée par la loi n° 2004-801du 6 août 2004, articles 226-16 et suivants du Code pénal) ;

**6. Textes généraux relatifs à l'utilisation de l'informatique et des réseaux** (loi n° 2004-575 du 21 juin 2004 relative à la confiance dans l'économie numérique) ;

**7. Textes relatifs à la preuve électronique** : article 1316-4 et suivants du Code civil (introduit par la loi n° 2000-230), décrets n° 2001-272 du 30 mars 2001 et n° 2002-535 du 18 avril 2002 ;

**8.** Décret n° 2006-358 du 24 mars 2006 relatif à **la conservation des données des communications électroniques**

**9.** Tous les textes relatifs au **droit à la vie privée**, à la **réputation** et à **l'image personnelle** dans le domaine public qui ne sont pas particulièrement ciblés sur l'utilisation des systèmes informatiques mais d'usage général.

**10.** Règlement européen n° 2016/679, relatif à la protection de données personnelles **(RGPD)**

# Adhésion à la charte

Document à rendre rempli et signé, puis remettre dans le dossier d'inscription

Elève / Etudiant(e) :

Je soussigné(e), Nom :……
Prénom :……. , agissant en qualité d'élève / Etudiant dans la classe de …….. , déclare par la présente avoir pris connaissance des 6 pages de la Charte d'utilisation des ressources informatiques de l'EPLEFPA du Bourbonnais, en avoir compris les termes et recommandations, et m'engage à les respecter.

Date :

Signature de l'apprenant:

Parents : Si l'élève / Etudiant est mineur(e) !

Nom :……..

Prénom……..

Date :……

Signature du responsable légal :……

*(ne dispense pas l'élève/ Etudiant mineur concerné de lire, signer et adhérer par contrat moral à cette charte)*