

# Charte Informatique 2020-2021

## 1. Domaines d'application

Ces règles s'appliquent à toute personne utilisant les systèmes informatiques de l'Ecole Notre-Dame "Les Oiseaux" et les systèmes informatiques auxquels il est possible d'accéder à partir de l'établissement. Ces systèmes comprennent notamment :

- des salles équipées d'ordinateurs et d'imprimantes,
- des tablettes,
- des postes de travail administratifs,
- des classes mobiles,
- des postes et ordinateurs mobiles,
- des matériels mis à disposition des utilisateurs,
- des ordinateurs ou autres appareils personnels utilisant les ressources de l'établissement (réseau filaire ou Wifi).

On appelle "**Utilisateur**" toute personne, quel que soit son statut (étudiant, enseignant, chercheur, ingénieur, administratif, personnel temporaire, stagiaire, ...) appelée à utiliser les ressources informatiques et les réseaux de l'établissement.

## 2. Conditions d'accès aux ressources informatiques et aux réseaux

L'utilisation des moyens informatiques et des réseaux de l'Ecole Notre-Dame "Les Oiseaux" doit être limitée à des activités administratives, de recherche, d'enseignement et de formation, de gestion ou de vie de l'établissement.

**L'utilisateur ne peut pas connecter un équipement informatique aux ressources informatiques et aux réseaux de l'établissement sans autorisation préalable.**

**L'utilisateur doit respecter les modalités de raccordement des matériels aux réseaux de communication telles qu'elles lui sont précisées par le responsable des moyens informatiques. Ces raccordements ne pourront pas être modifiés sans autorisation préalable.**

L'utilisateur est responsable de l'utilisation des ressources informatiques (locales ou distantes) effectuée à partir de son droit d'accès. Conformément aux lois en vigueur, et notamment à la loi **DADVSI**, l'utilisateur doit pouvoir être identifié par l'administrateur. Tous les « logs » de l'utilisateur sont conservés durant une période d'une année, et pourront être utilisés en cas de litige.

**Les personnes apportant leur propre matériel doivent en informer le responsable des moyens informatiques. Pour assurer la sécurité des systèmes, il devra alors lui communiquer toutes les informations nécessaires à son identification sur le réseau.**

Les données enregistrées sont conservées par les services informatiques dans le respect de la Loi (RGPD) et conformément aux directives de la CNIL.

**Le droit d'accès est temporaire; il est retiré dans les cas suivants :**

- la fonction de l'utilisateur ne le justifie plus ;
- le non-respect du présent règlement.

*L'utilisateur accepte les droits de l'administrateur tels qu'ils sont définis en article 4.*

### **3. Respect des principes de fonctionnement des systèmes informatiques**

#### **3.1 - Sécurité informatique**

L'utilisateur est tenu de participer à la sécurité du système (choix de mots de passe solides, protection de son espace de stockage, signaler tout problème de sécurité, ...)

L'utilisateur ne doit pas effectuer de manœuvre qui aurait pour objet de **méprendre les autres utilisateurs sur son identité**. L'utilisateur doit respecter les procédures d'authentification en vigueur de façon à ce que les actions qu'il mène au sein des systèmes soient identifiables.

L'utilisateur ne doit pas effectuer d'expérimentation sur la sécurité des systèmes informatiques et des réseaux, ni sur les virus informatiques sans autorisation préalable. Le développement, l'installation ou la simple détention d'un programme ayant les propriétés décrites ci-dessous sont également interdits :

- programmes cherchant à contourner la sécurité d'un système ;
- programmes contournant les protections des logiciels.

Tout utilisateur d'un réseau informatique s'engage à ne pas effectuer d'opérations qui pourraient avoir pour conséquence :

- d'interrompre le fonctionnement du réseau ou d'un système connecté au réseau ;
- d'accéder aux informations privées d'autres utilisateurs sur le réseau ;
- de modifier ou de détruire des informations sur un des systèmes connectés au réseau ;
- de nécessiter la mise en place de moyens humains ou techniques supplémentaires pour son contrôle.

#### **3.2 Gestion des ressources**

L'utilisateur doit respecter les règles et procédures mises en place pour l'acquisition et la sortie des données sur les machines de l'établissement. Il respectera les procédures et restrictions d'acquisition/extraction des données à partir des supports électroniques. Ceci concerne principalement les accès téléinformatiques (téléchargements à partir du Cloud) et les supports amovibles (clefs USB, cards, disquettes, bandes, etc.).

L'utilisateur ne doit utiliser que les ressources pour lesquelles il a eu une autorisation d'usage. Ceci est valable aussi bien pour les points d'accès, que pour les périphériques (imprimantes, vidéo projecteurs, traceurs,...).

L'utilisateur ne pourra pas ainsi utiliser les logiciels de dialogue en ligne durant la journée. L'utilisateur est tenu de participer à l'exploitation des ressources en se conformant aux directives d'exploitation précisant les modalités d'accès et de partage de ces ressources. Le développement, l'installation, ou la simple détention d'un programme saturant les ressources (informatiques et/ou réseaux) sont également interdits.

### **3.3 Respect d'un comportement correct**

L'utilisateur ne doit pas utiliser les systèmes informatiques pour harceler d'autres utilisateurs par des communications non souhaitées par les tiers ou pour afficher/diffuser des informations illégales.

Il est rappelé que des lois plus générales et notamment le Code Pénal s'appliquent pour des informations ou messages :

- à caractère injurieux,
- à caractère pornographique,
- à caractère diffamatoire,
- d'incitation au racisme,
- etc.

Les lois s'appliquent de la même manière quant aux publications sur des sites, blogs ou réseaux sociaux. Y enfreindre les droits d'autrui est passible de poursuites civiles et pénales.

### **3.4 Règles à respecter lors des visioconférences.**

Pour rappel, une visioconférence permet à un groupe de personnes de communiquer via le son et l'image à distance, via un accès internet. C'est un moyen pratique pour organiser une réunion à distance.

Lors d'une séance de cours en distanciel, le règlement intérieur de l'établissement s'applique. Au même titre qu'en présentiel, l'assiduité et la ponctualité doivent être respectées par chacun. Les séances de visioconférence programmées par les enseignants sont obligatoires.

Une charte spécifique aux séances en visioconférence est disponible sur le site Internet de l'établissement ou sur simple demande à notre administration.

#### 4. Les droits de l'administrateur

L'administrateur est le responsable de la distribution et du retrait des droits d'accès.

L'administrateur doit faire respecter les droits et responsabilités des utilisateurs présents sur ses ressources. Il est un référent RGPD et fait appliquer les Lois et les recommandations et obligations fixées par la CNIL.

L'administrateur se réserve le droit de prendre toutes dispositions nécessaires pour assumer ses responsabilités et permettre le fonctionnement optimal des ressources informatiques qu'il a en charge. L'administrateur peut prendre des mesures "conservatoires" (arrêts de travaux, suppression de droits d'accès, verrouillage de fichiers, fermeture de salles...) en vue de :

- arrêter un engorgement de ses ressources ;
- figer un état lors de problèmes liés à la sécurité des systèmes informatiques ;
- figer un état lors de problèmes liés au comportement des utilisateurs.

L'administrateur peut :

- accéder à des fichiers ou des courriers en vue de réaliser un diagnostic, une correction d'un problème et/ou s'assurer du bon fonctionnement des ressources qu'il a en charge ;
- examiner des données utilisateurs en vue d'assurer la bonne marche du système qu'il a en charge et/ou de s'assurer du bon respect du règlement de la part des utilisateurs ;
- contrôler la bonne utilisation des ressources et prendre des décisions pouvant affecter l'espace fichier ou les travaux lancés par un utilisateur ;
- surveiller en détail les sessions de travail d'un utilisateur soupçonné de non-respect du présent règlement.

Tout utilisateur n'ayant pas respecté le règlement énoncé ci-dessus est passible de poursuites :

- internes à l'établissement ;
- pénales pour les infractions relevant du Nouveau Code Pénal.

Fait à Verneuil-sur-Seine, le 21 janvier 2021,

Le Chef d'Etablissement,  
Monsieur Yves LE SAOUT

Le Responsable Informatique,  
Monsieur Stéphane SCHAULER