DIRECTIVE POUR L'UTILISATION DES RESSOURCES INFORMATIQUES

TOUS LES TERMES UTILISÉS DOIVENT ÊTRE COMPRIS DANS LEUR SENS ÉPICÈNE.

1. INTRODUCTION

La présente directive a pour but de préciser les droits et les devoirs, le comportement et la responsabilité des utilisateurs du matériel informatique du ceff. Elle précise les attitudes personnelles et collectives à avoir pour préserver la sécurité informatique globale dans notre école.

Cette sécurité informatique est assurée par le service informatique du ceff. Elle consiste pour l'essentiel à interdire l'accès aux serveurs de données et d'applications aux personnes externes à l'école et à assurer la confidentialité des données à l'intérieur même de notre établissement.

Les utilisateurs sont les membres de la direction, du personnel administratif et technique, les enseignants et les élèves du ceff, y compris ceux de la formation continue. Par ressources informatiques, on entend notamment le matériel, les logiciels informatiques ainsi que les accès au réseau local et à Internet.

2. COMPORTEMENT ET RÈGLES D'UTILISATION DES RESSOURCES INFORMATIQUES

2.1. GÉNÉRALITÉS

- Seules les personnes ayant lu, compris et accepté le présent document ont accès aux ressources informatiques du ceff. Le délai d'acceptation est de trois mois après l'ouverture du compte informatique, faute de quoi le compte informatique sera bloqué.
- L'utilisateur respecte et utilise avec soin le matériel mis à sa disposition.
- L'utilisateur prévient immédiatement le service informatique pour tout incident ou disfonctionnement constatés.
- La consommation de boissons et de nourriture n'est pas autorisée dans les salles d'informatique.
- Les ressources informatiques ne doivent être utilisées que dans le strict cadre de la formation ou des obligations professionnelles des utilisateurs. Une utilisation privée peut toutefois être tolérée pour autant qu'elle ne perturbe pas le bon fonctionnement du système et qu'elle ne vise aucun but lucratif. Le ceff ne peut pas être tenu pour responsable en cas de diffusion de données personnelles.

2.2. CONFIGURATION DES ORDINATEURS

- Aucune modification de configuration (matériel et logiciel) des ordinateurs n'est autorisée sans l'accord préalable du service d'informatique.
- L'utilisateur veille à ne pas introduire de virus dans le réseau par des manipulations inadéquates.
- Sur les ordinateurs qui ne sont pas gérés par le service informatique (ateliers informatique et ordinateurs privés), l'utilisateur s'assure qu'un logiciel antivirus est installé et à jour.

2.3. ORDINATEUR PERSONNEL

- Le type d'appareil est défini par le service informatique en fonction des besoins des utilisateurs. Le droit d'accès « administrateur » est possible pour l'utilisateur.
- L'appareil mis à disposition reste la propriété du ceff. Il peut être repris à tout moment en cas de besoin, mais l'utilisateur en sera averti préalablement et le service informatique assurera la transition.
- Le possesseur d'un ordinateur personnel assume l'entière responsabilité en cas de dommage volontaire ou par négligence grave

2.4. LOGICIELS

- Tous les logiciels disponibles au ceff sont répertoriés dans le « centre logiciel » ainsi que dans le partage P:\Logiciels. Au besoin, l'utilisateur peut prendre contact avec le service informatique pour savoir quel logiciel répond à un besoin particulier et si nécessaire, discuter des modalités d'acquisition.
- Tous les logiciels acquis par le ceff le sont pour une utilisation exclusive au ceff. Il est interdit d'en faire une copie pour une utilisation externe au ceff, à l'exception des logiciels spécifiquement prévus pour une utilisation personnelle (voir page intranet « pour la maison »)

2.5. DROITS D'AUTEUR

- Il est interdit de télécharger, transférer ou copier des logiciels, de la musique, des films, des images ou tout autre média protégés par des droits d'auteur pour lequel l'utilisateur ne possède pas de droit.

2.6. MOT DE PASSE

Le mot de passe est nécessaire pour sécuriser l'ensemble du système informatique ; il permet de protéger l'utilisateur et lui donne accès à certaines applications et certaines données.

- Le mot de passe rend responsable l'utilisateur de tous ses actes.
- Le mot de passe est une information personnelle qui ne doit en aucun cas être transmise à autrui ni écrite quelque part.
- L'utilisateur ne se sert pas d'un compte qui ne lui appartient pas.

- En cas d'absence, l'utilisateur verrouille son poste de travail.
- L'utilisation d'un code PIN ou d'une empreinte digitale est autorisée comme moyen d'authentification local.

2.7. PROTECTION ET UTILISATION DES DONNÉES

Le ceff gère les données des élèves dans le respect de la législation. Conformément à la loi cantonale sur la protection des données, il est possible que certaines informations soient publiées dans des annuaires à usage interne ou transmises à diverses autorités.

Les utilisateurs ont accès à certaines données spécifiques au ceff (supports de cours, liste d'adresses, bases juridiques, procédures et processus, projets, notes, résultats d'examens, etc.). La règle de base est de considérer toutes ces données comme étant la propriété du ceff. Aucune de ces données ne peut être mise à disposition de personnes externes à l'école sans l'accord express de la direction du ceff ou de la direction d'un domaine. En particulier, les utilisateurs :

- s'engagent à ne pas diffuser des éléments qui peuvent ternir la réputation d'un élève, d'un enseignant, d'un membre du personnel ou de la direction du ceff ou de l'institution elle-même ainsi qu'à respecter la sphère privée, la personnalité et l'image de chacun ;
- s'engagent à ne pas consulter, enregistrer ou diffuser des documents qui portent atteinte à la dignité de la personne, présentent un caractère pornographique, incitent à la xénophobie ou à la haine raciale ou constituent une apologie du crime ou de la violence (articles 173 et suivants, 197 et 261 du Code pénal suisse).

2.8. ABSENCE / DÉPART / DÉCÈS

En cas d'absence prolongée d'un collaborateur, sur décision de la Direction, ses données personnelles peuvent être transmises à son supérieur.

En cas de départ volontaire ou non, le collaborateur dépose ses données personnelles dans les emplacements communs et met tout en œuvre pour que son successeur ait tous les documents nécessaires à disposition. Sur demande des Ressources humaines, une réponse automatique est mise en place pour la messagerie de la personne ayant quitté le ceff.

Dès l'annonce officielle d'un décès par la Direction et sur décision de la Direction, les données du défunt sont transmises à son supérieur. Sur demande des Ressources humaines, une réponse automatique est mise en place pour la messagerie du disparu.

2.9. MESSAGERIE ET ESPACE DE STOCKAGE

La messagerie étant la principale méthode de contamination de virus informatiques, l'utilisateur s'assure, avant d'ouvrir un message qu'il n'est pas douteux et qu'il provient d'un correspondant connu.

L’utilisateur se sert de la messagerie ainsi que de son espace de stockage personnel (lecteur U:\) ou de l’espace partagé pour des raisons professionnelles et réduit au minimum son utilisation privée. Seul le contenu des emplacements de stockage du ceff est sauvegardé par le service informatique.

Le stockage de données sur le cloud Microsoft, Onedrive, est assuré et accessible en tout temps à l’adresse onedrive.com. En cas de suppression, les données sont sauvegardées durant 30 jours, après quoi, il n’est plus possible de les récupérer.

Les élèves ne sont pas autorisés à utiliser les listes de distribution figurant dans Outlook. Les demandes de participation à un sondage ou à un questionnaire doivent faire l’objet d’un communiqué dans l’Intranet, après accord du Directeur de domaine concerné.

2.10. INTERNET

Les utilisateurs :

- fréquentent internet pour des raisons scolaires ou professionnelles. L’accès pour des besoins privés est permis avec modération uniquement sur les temps de pauses ;
- ne fréquentent aucun site à contenu illicite ou contraire aux bonnes mœurs.

2.11. IMPRIMANTES ET COPIEURS

Les utilisateurs :

- évitent de lancer des impressions longues pendant les heures de travail, afin de ne pas bloquer l’accès pour les autres utilisateurs. Il est conseillé de faire les impressions de plus de 50 pages sur les copieurs qui sont plus adaptés ;
- retirent de l’imprimante ou des copieurs toutes les impressions envoyées.

En règle générale, les utilisateurs impriment uniquement des documents en lien avec leur activité au ceff. Exceptionnellement, ils peuvent imprimer ou copier des documents privés. Ils doivent dès lors rembourser le coût correspondant selon le tarif des émoluments.

2.12. VPN, CONNEXION DEPUIS L’EXTERIEUR DU CEFF

Les utilisateurs bénéficient de la possibilité de se connecter au réseau informatique du ceff depuis l’extérieur, moyennant la mise en place d’un VPN. Toutefois, l’utilisateur doit s’assurer :

- avoir effectué les mises à jour de son ordinateur ;
- que son ordinateur est équipé d’un anti-virus à jour.

2.13. OUTIL DE SURVEILLANCE DES ORDINATEURS DE LA CLASSE

Les enseignants des salles d'informatique et des ateliers ont à disposition un outil de surveillance des ordinateurs de la classe. Cet outil permet, par exemple, de voir les pages Internet visitées, le programme en cours, les écrans des élèves et de bloquer certains éléments de l'ordinateur (USB, imprimante, Internet, programmes, …).

L'enseignant peut utiliser cet outil afin de contrôler sporadiquement l'utilisation des ressources informatique par ses élèves. Le contrôle peut se faire lorsque l'enseignant est en classe avec ses élèves ou depuis une autre classe (par exemple depuis une classe de théorie alors que ses élèves sont dans la classe de pratique). L'outil n'effectue pas de journalisation et ne permet pas de prendre à distance le contrôle de la caméra ni du microphone.

3. MESURES DE PROTECTION ET JOURNALISATION

3.1. MESURES DE PROTECTION TECHNIQUES

Le ceff met en œuvre les mesures de protection techniques suivantes :

- Antivirus à jour sur les postes de travail et les serveurs
- Accès Internet sécurisé (filtre de contenu, interception SSL, antivirus)
- Filtrage des courriels
- Droits d'administration limités
- Contrôle des ordinateurs des salles d'informatiques et des ateliers
- Restriction de l'accès physique aux bâtiments/salles

3.2. JOURNALISATION

Des fichiers journaux sont générés pour la plupart des activités réalisées à l'aide de moyens informatiques. Cela consiste à enregistrer les informations de type : « Qui, Quoi, Quand ». Au sein du ceff, la journalisation est opérée pour les services suivants :

- Accès à Internet
- Impressions
- Accès à la messagerie (webmail, outlook, activesync)
- Envoi/Réception de courriels
- Connexion/Déconnexion des ordinateurs
- Connexions VPN
- Accès Wifi
- Accès aux salles disposant d'une serrure électronique

4. RESPONSABILITÉ ET SANCTIONS

Chaque utilisateur est responsable de l'usage qu'il fait des ressources informatiques du ceff, ainsi que de l'ensemble des informations qu'il met à disposition du public.

Le ceff prendra les mesures administratives et/ou disciplinaires en cas de violation de la présente directive. Demeure réservé l'engagement de poursuites pénales et/ou civiles.

Il est en outre rappelé que la législation s'applique également pleinement en matière informatique, notamment le code pénal (en particulier les art. 173 et suivants qui concernent les infractions contre l'honneur), le code civil (en particulier les art. 28 et suivants s'agissant des atteintes à la personnalité) et la loi sur le droit d'auteur.

La présente directive s'applique également aux personnes qui reçoivent du matériel informatique et des accès à notre système informatique précédemment à leur engagement formel au ceff. Celles-ci sont en outre soumises au secret de fonction tel que décrit par la Loi sur le personnel (LPers ; RSB 153.01).

Enfin, la charte interne d'utilisation des réseaux sociaux est également applicable et fait partie intégrante de la présente directive.

La présente directive entre en vigueur le 15 juin 2021. Elle remplace et annule la version du 1er août 2020.

St-Imier, le 9 juin 2021

Cédric Bassin

Directeur général