DIRECTIVE POUR L'UTILISATION DES RESSOURCES INFORMATIQUES

TOUS LES TERMES UTILISES DOIVENT ETRE COMPRIS DANS LEUR SENS EPICENE.

1. INTRODUCTION

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

La sécurité informatique est assurée par le service informatique du ceff. Elle consiste, pour l'essentiel, à contrôler et superviser l'accès aux ressources informatiques et interdire tout accès non autorisé.

Cette directive s'adresse à toutes les personnes, collaborateurs, élèves, visiteurs qui utilisent les ressources informatiques du ceff (applications, wifi, messagerie, ordinateurs, accès internet, etc.).

2. COMPORTEMENT ET REGLES 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 d'un mois après le début de l'activité au ceff, 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 dysfonctionnement constaté.
- La consommation de boissons ou de nourriture n'est pas autorisée à proximité du matériel informatique et 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.

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 programme malveillant de manière volontaire ou non.
- Sur les ordinateurs qui ne sont pas gérés par le service informatique (ateliers informatique, ordinateurs privés, certain labo, etc.), l’utilisateur s’assure que son ordinateur ne présente pas de risque pour les systèmes d’information du ceff. Pour ce faire, l’antivirus, le système d’exploitation et toutes les applications installées doivent être à jour.

2.3. ORDINATEURS ATTRIBUÉS NOMINATIVEMENT

- Les ordinateurs attribués nominativement à un collaborateur sont sous la responsabilité du collaborateur.
- Le type d’ordinateur est défini par le service informatique en fonction des besoins des utilisateurs et du stock disponible.
- L’ordinateur mis à disposition reste la propriété du ceff. Il peut être repris à tout moment sans justification. Dans ce cas, le service informatique veillera à ce que l’utilisateur puisse réaliser ses tâches professionnelles avec un ordinateur de remplacement.
- Aucune sauvegarde n’est réalisée sur l’ordinateur attribué. Il incombe à l’utilisateur de sauvegarder ses données aux emplacements dédiés à cet effet.
- Le possesseur d’un ordinateur personnel assume l’entière responsabilité en cas de dommage volontaire ou causé par négligence.

2.4. ORDINATEURS APPORTÉS PAR LES ÉLÈVES « BYOD »

- Sur les ordinateurs BYOD, un programme est installé pour vérifier la compatibilité de l’ordinateur avec les besoins d’utilisation au ceff. Ce programme collecte des informations propres à l’ordinateur. Conformément à la l’art. 8 LPD, sur demande au service informatique, l’élève peut demander une liste des données collectées sur son ordinateur personnel.
- Une fois l’ordinateur intégré dans le programme BYOD, il est possible que l’installation de certains logiciels soit proposée ou imposée pour les besoins de l’enseignement.
- Il est de la responsabilité de l’élève de supprimer tous les programmes et licences installés sur l’ordinateur BYOD à la fin de sa formation au ceff.
- Aucune sauvegarde n’est faite sur les ordinateurs BYOD.
- L'accès aux ordinateurs BYOD doit être sécurisé par un moyen adéquat (mot de passe, biométrie, etc.). Le système d’exploitation et les logiciels doivent être mis à jour régulièrement. De plus, un antivirus doit être installé et configuré pour une mise à jour régulière et automatique.
- Le service informatique se réserve le droit de supprimer et d’interdire l’accès au réseau informatique du ceff, sans préavis, à tout ordinateur BYOD qui serait identifié comme un risque pour la sécurité du système d’information.

2.5. LOGICIELS

- Tous les logiciels disponibles au ceff sont répertoriés dans la liste des applications homologuées disponibles dans l'intranet sous la rubrique « service informatique ».
- Tous les logiciels acquis par le ceff le sont pour une utilisation exclusivement professionnelle dans le cadre de l'activité de l'utilisateur au ceff.

2.6. DROITS D'AUTEUR

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

2.7. 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'une solution biométrique est autorisée comme moyen d'authentification local.
- Pour garantir l'identité de l'utilisateur, une solution de double authentification (MFA) peut être requise. Ceci implique l'envoi de SMS ou l'utilisation d'une application sur le téléphone mobile de l'utilisateur.

2.8. PROTECTION ET UTILISATION DES DONNÉES

Le ceff gère les données des élèves dans le respect de la législation. Conformément à la législation 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.). Toutes ces données sont la propriété du ceff et ne peuvent être mises à disposition de personnes externes à l'école sans l'accord écrit de la direction générale 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 (art. 173 et suivants, 197 et 261 du Code pénal suisse).

2.9. ABSENCE / DEPART / DECES

En cas d’absence prolongée d’un collaborateur, sur décision de la direction générale, ses données enregistrées dans les espaces de stockage du ceff peuvent être transmises à son supérieur.

En cas de départ volontaire ou non, le collaborateur dépose ses données 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 générale et sur décision de celle-ci, 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.

2.10. 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. Dans le doute, il contacte le service informatique avant d’ouvrir le message.

L’utilisateur se sert de la messagerie ainsi que de son espace de stockage personnel ou partagé pour des raisons professionnelles et réduit au minimum son utilisation privée. Les espaces de stockage et la messagerie sont sauvegardés avec un historique de 30 jours.

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.

2.11. INTERNET

Les utilisateurs :

- fréquentent internet pour des raisons scolaires ou professionnelles. L’accès pour des besoins privés est toléré dans la mesure où cela n’interfère pas avec le bon fonctionnement de l’établissement ;
- ne fréquentent aucun site à contenu illicite ou contraire aux bonnes mœurs ;

- ne donne pas des accès à des personnes ou à des systèmes aux ressources informatiques du ceff, de manière volontaire ou non, à travers la connexion internet mise à disposition.

Tous les accès à internet fait depuis le réseau du ceff ou depuis un ordinateur propriété du ceff peuvent être enregistré sans préavis (voir ch. 3 Journalisation).

2.12. IMPRIMANTES ET COPIEURS

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.

Pour certaines catégories d'utilisateurs, l'impression est dans tous les cas facturée. Les utilisateurs concernés sont informés directement.

2.13. VPN, CONNEXION DEPUIS L'EXTERIEUR DU CEFF

Certains 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 antivirus à jour.

Le service informatique se réserve le droit de supprimer et d'interdire l'accès au VPN ou les connexions depuis l'extérieur du ceff, sans préavis, à tout ordinateur ou utilisateur qui serait identifié comme un risque pour la sécurité du système d'information du ceff.

2.14. 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, etc.).

L'enseignant peut utiliser cet outil afin de contrôler sporadiquement l'utilisation des ressources informatiques 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. 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 peut être opérée sur tous les systèmes, entre autres pour les services suivants :

- accès à Internet
- impressions
- accès à la messagerie
- envoi/réception de courriels
- connexion/déconnexion des ordinateurs
- connexions VPN
- accès Wifi
- accès aux salles disposant d'une serrure électronique

À la demande de la direction générale ou de la direction des domaines, un rapport de journalisation sur un composant pendant une période peut être demandé au service informatique.

4. RESPONSABILITE 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 de tiers. Des sanctions administratives et/ou disciplinaires peuvent être prises 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 1er août 2023. Elle remplace et annule la version du 15 juin 2021.

St-Imier, le 14 juin 2023

Cédric Bassin

Directeur général