

Charte informatique

Division artisanale du CEJEF

V. 2026-0.1

CHARTRE INFORMATIQUE

1. Préambule

Les termes utilisés pour désigner des personnes s'adressent indifféremment aux femmes et aux hommes. Pour faciliter la lecture, le genre masculin a été retenu.

2. Définitions

On entend par **ressources** tous les outils informatiques permettant un échange d'informations, tels que notamment les matériels, réseaux, serveurs, ordinateurs, portables, imprimantes, logiciels, fichiers, services Intranet ou Internet (sites Web, messagerie, transfert de fichiers, forums).

Le terme **utilisateur** désigne toute personne qui fréquente une division du CEJEF utilisant ou ayant accès aux ressources informatiques et/ou se rendant sur des médias sociaux.

Les données servant à identifier un utilisateur dans le système informatique, comme son nom d'utilisateur et son mot de passe, constituent son **compte** d'utilisateur.

3. Champs d'application et objectif

Les règles et obligations énoncées ci-dessous s'appliquent aux élèves, aux personnes en formation, aux enseignants, aux animateurs de cours et au personnel administratif et technique. Cette charte définit les points à respecter et prévient les utilisateurs des conséquences pouvant découler d'une utilisation inappropriée du matériel et logiciel informatiques contraire aux directives qu'elle contient.

Par cette démarche, le Centre jurassien d'enseignement et de formation (CEJEF) et ses divisions marquent leur volonté d'encadrer l'usage de l'informatique et des réseaux sociaux.

4. Directives générales

Les directions de divisions définissent les ressources mises à disposition de chaque utilisateur.

L'utilisation des ressources n'est autorisée que dans le cadre de l'administration, de la gestion et de la formation dispensée ou reçue au sein d'une division. Lors de temps sans période d'enseignement, les enseignants peuvent utiliser le matériel à des fins privées, mais de manière limitée. Aucun usage commercial ou lucratif n'est autorisé. Il est de plus interdit d'accéder à des jeux en ligne, de consulter des forums, de télécharger des jeux, des fichiers musicaux ou des vidéos sans lien direct avec la formation.

Chaque utilisateur doit prendre le plus grand soin des ressources mises à sa disposition. Les divisions ne reconnaissent aucune responsabilité ou obligation d'entretien pour les ressources privées amenées en leur sein, même si celles-ci sont utilisées dans le cadre des activités scolaires.

5. Conditions d'accès aux réseaux informatiques

Pour avoir accès aux ressources informatiques de sa division, chaque utilisateur doit prendre connaissance de cette charte. Il se voit attribuer un identifiant et un mot de passe lui permettant de :

- se connecter aux serveurs informatiques de la division ;
- utiliser les ressources informatiques et pédagogiques disponibles ;
- accéder aux informations et ressources présentes sur le réseau Internet.

Les codes d'accès attribués sont strictement personnels. Il est interdit à l'utilisateur de :

- communiquer les données de son compte, ou son mot de passe personnel à quiconque ;
- utiliser un compte d'utilisateur autre que le sien ;
- masquer sa véritable identité lors d'accès informatiques ;
- quitter un poste de travail informatique sans se déconnecter ou le verrouiller.

L'utilisateur doit impérativement :

- signaler à la direction de sa division toute tentative d'utilisation ou de violation de son compte ou de ses fichiers propres ;
- être conscient qu'il est responsable de tout ce qui est fait sous le couvert de son compte.

6. Utilisation des ressources et des données informatiques

Chaque utilisateur est responsable de l'usage qu'il fait des ressources informatiques. Le matériel informatique doit être manipulé avec précaution et soin, en respectant les points suivants :

- quitter correctement les logiciels utilisés ou verrouiller le poste de travail durant la pause ;
- arrêter les postes de travail et les périphériques en fin de session ;
- se montrer très prudent lors de la réception de messages douteux ;
- veiller à ne pas surcharger le réseau, en particulier par des téléchargements de fichiers volumineux ou par le lancement de procédures lourdes.

En tant qu'utilisateur, il convient de se rappeler qu'il est notamment interdit de :

- recopier ou emprunter des logiciels appartenant à la division ;
- installer des logiciels sans autorisation du responsable informatique ;
- installer des logiciels à caractère ludique ou s'apparentant à des virus ;
- contourner les restrictions d'utilisation d'un logiciel ;
- interrompre ou perturber volontairement le fonctionnement du réseau ;

- modifier ou détruire des informations sur le système ;
- modifier une configuration, un câblage ou les attributs de fichiers sans autorisation;
- débrancher un périphérique sans autorisation ;
- déplacer les périphériques et accessoires équipant le poste de travail ;
- tenter de lire, modifier, déplacer, copier ou supprimer sans autorisation des fichiers appartenant à d'autres utilisateurs ;
- rendre des données confidentielles accessibles à des personnes tierces ;
- installer ou copier des fichiers musique, vidéo, film, jeux ou démos autres que ceux nécessaires au déroulement de la formation ;
- installer ou copier dans les ordinateurs des fichiers image ou photo autres que ceux nécessaires au déroulement de la formation ;
- commettre une infraction pénale à l'aide des ressources mises à disposition.

7. Utilisation de clés USB

Dans la mesure où l'utilisation des clés USB représente une faille de sécurité importante, elle est strictement interdite sur l'ensemble du matériel informatique. Par le biais M365, les divisions du CEJEF offrent aux utilisateurs une alternative fiable et diverse de partage ou de stockage de documents.

8. Utilisation d'Internet

Dans le cadre de l'utilisation d'Internet, il est strictement interdit de consulter des sites :

- sans rapport avec la recherche demandée par l'enseignant ou le travail réalisé dans le cadre des études ;
- à caractère raciste, violent, xénophobe ou pornographique selon la loi fédérale (art. 197 Code pénal).

Il est également interdit d'utiliser Internet pour commettre une infraction pénale, notamment en diffusant des injures, des calomnies ou des diffamations.

9. Contrôles et moyens de preuve

Pendant les périodes d'enseignement, toutes activités (accès aux applications, accès internet, impressions et autres) peuvent faire l'objet d'une surveillance en cas de fonctionnement anormal et/ou douteux.

Le service informatique de la division tient un inventaire des utilisateurs et des ressources mises à disposition.

Le personnel administratif est soumis aux directives relatives à l'usage des ressources informatiques et de la télécommunication.

10. Médias sociaux

Les médias sociaux sont des outils de discussion, d'échange et de partage. Ceux-ci regroupent une grande variété d'applications différentes.

Les divisions du CEJEF, sauf circonstance particulière de formation autorisée par la direction, n'ouvrent pas l'accès aux médias sociaux et en interdisent, de fait, l'usage. Cependant, l'accès à ces applications est autorisé pour autant qu'il y ait un lien avec l'enseignement et la formation.

En cas d'accès autorisé, l'utilisateur respectera les règles déontologiques ci-après :

L'utilisateur doit utiliser les médias sociaux selon des règles éthiques et morales.

Entre autres, il :

- s'engage à ne pas porter atteinte à la personnalité d'une personne, notamment par l'intermédiaire de messages, de textes ou d'images provocantes ;
- respecte la vie privée des personnes ;
- assume l'entière responsabilité de ce qu'il écrit, que ce soit sur son site personnel ou sur les autres sites (tout ce qui est écrit et/ou publié sur Internet est accessible pendant un certain temps. Même si un contenu est supprimé, il peut être retrouvé) ;
- respecte le droit à l'image; toute publication de photo requiert l'autorisation de qui de droit ;
- ne poste pas d'information sur la division concernant son organisation, ses formations, ses élèves et le personnel enseignant et/ou administratif. Le secret de fonction et les règles sur la protection des données (CPDT-JUNE) doivent être scrupuleusement respectées ;
- respecte le droit d'auteur. Dans le cadre des travaux à effectuer durant le cursus de formation, il devra citer ses sources de manière complète.

11. Byod - Ordinateur personnel

Comme précisé dans le contrat de formation, les personnes utilisant un ordinateur portable privé seront soumises à l'installation d'un logiciel de surveillance sur leur matériel. Ce logiciel ne sera actif qu'à l'utilisation des réseaux WIFI du CEJEF. Il sera donc exigé d'utiliser ces derniers dans les différentes divisions, excluant de facto le recours au partage de connexion privé.

En outre, chaque division du CEJEF se réserve le droit d'opter pour une stratégie d'équipement numérique qui lui est propre et de déterminer des exigences techniques minimales.

12. Sanctions

Tous les comportements considérés comme inadéquats sont décrits en détail dans les paragraphes précédents. Les personnes ne respectant pas les directives indiquées s'exposent à différentes sanctions qui peuvent aller jusqu'à l'exclusion du CEJEF (RSJU 412.11 LEST art. 63).

D'autre part, les divisions n'assument aucune responsabilité en cas d'utilisation abusive de leurs ressources à leur insu : elles se dégagent d'éventuelles poursuites pénales en cas de découverte d'utilisation illégale ou non autorisée de leur système informatique.

En cas de perte du « login » ou du mot de passe, un montant de **CHF 10.-** sera demandé à l'élève.

13. Compte MICROSOFT 365 ET MESSAGERIE professionnelle

Une adresse mail est créée pour chaque apprenti/étudiant du CEJEF. La messagerie est un outil de communication moderne important. Il convient à chaque élève de relever au moins deux fois par semaine sa boîte mail. L'utilisation de l'adresse mail de division est réservée à l'usage professionnel/scolaire uniquement.

14. DISPOSITIONS FINALES

De par sa signature au bas du contrat de formation, chaque élève s'engage à respecter les directives de la présente charte informatique.

La direction de la DivArt