CHARTE D'USAGE DES OUTILS ET SERVICES NUMÉRIQUES
PAR LES APPRENANTS DU CFA DE SAÔNE-ET-LOIRE – SITE DE [NomDuSite]

Sommaire

PRÉAMBULE

La fourniture des services numériques et l'accès aux Technologies de l'Information et de la Communication pour l'Enseignement (TICE) font partie intégrante de la mission de service public de l'éducation. L'usage des services et outils numériques s'exerçant dans un cadre légal et réglementaire doit en conséquence être régulé. 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.
La présente charte a pour objet de répondre à ce double objectif de sensibilisation et de régulation. Elle vise à :

- fixer les règles relatives à l'utilisation des locaux et ressources informatiques
- fixer les règles relatives à la gestion des données personnelles de l'utilisateur (déclinaison du RGPD dans l'établissement)
- préciser les modalités de la sensibilisation et de l'éducation aux outils et services numériques
- déterminer les engagements de l'utilisateur et de l'établissement
- préciser les modalités des éventuels contrôles portant sur l'utilisation des services proposés

La charte comporte en annexe un glossaire des termes techniques pour que leur signification soit partagée par l'ensemble de la communauté éducative.

1. Le périmètre de la charte

1.1. Les utilisateurs concernés

Les dispositions de cette charte s'appliquent à tous les apprenants qu'ils soient internes, externes ou demi-pensionnaires y compris ceux présents occasionnellement et ceux originaires d'autres établissements.

1.2. Les lieux et services concernés

La charte s'applique :

1. dans l'ensemble des lieux relevant du CFA de Saône-et-Loire (multi sites, internat, atelier technologique, exploitation agricole, etc…)
2. à l'ensemble des services et outils numériques mis à disposition de l'utilisateur.

Liste des services et outils numériques concernés : ENT, PC, Photocopieurs, logiciels, salle informatique, messagerie électronique, services attachés à l'accès internet, etc…

Sauf dérogation, les dispositions de la charte sont applicables à l'ensemble des activités organisées par l'établissement dans ses locaux ou à l'extérieur de ces derniers (voyages organisés par exemple).

2. Les règles relatives à l'utilisation des locaux et des ressources informatiques

Par ressources informatiques, il faut entendre les matériels ou services (messagerie, ENT, accès internet, etc.…)

Le CFA de Saône-et-Loire met à disposition de ses utilisateurs du matériel informatique destiné à leur usage dans le cadre de leur activité au sein de l'établissement : micro-ordinateurs ainsi que leurs périphériques, des réseaux pédagogiques et Administratifs. L'utilisation du réseau peut être affectée à une personne, en libre service ou faire partie d'une salle de formation. Il permet d'accéder à des informations, à des logiciels et/ou à Internet. L'utilisation des ressources informatiques et Internet est soumise au respect du règlement intérieur. Il est précisé que l'utilisation de l'informatique au sein de l'établissement est strictement réservée à des fins pédagogiques et que l'utilisation de l'Internet s'inscrit obligatoirement dans le cadre de travaux éducatifs et de recherches programmés, à caractère pédagogique, en liaison avec un membre de l'équipe pédagogique.

Pour des raisons pratiques, les formateurs et les administrateurs ont accès aux espaces de stockage des salles de formation et aux espaces de stockage des apprenants, à l'exception du dossier personnel.

Chaque utilisateur s'engage à prendre connaissance et à respecter toutes les règles spécifiques à certains lieux pour l'utilisation des moyens informatiques (exemple : CDI, Foyer…)

Chaque utilisateur s'engage à prendre soin du matériel et des locaux informatiques mis à sa disposition. Il informera le responsable (formateur, surveillant…) ou l'administrateur réseau de toute anomalie constatée.

L'utilisateur doit impérativement fermer sa session de travail avant de quitter l'ordinateur.

2.1. Conditions d'accès aux matériels et services informatiques

L'établissement fait bénéficier l'utilisateur d'un accès aux ressources informatiques suivantes :

- ➔ Accès Internet :
  - ▸ L'utilisateur ne doit en aucun cas :
    - ▪ procéder à l'installation d'un logiciel sur un ordinateur du réseau et le rendre accessible sans accord préalable d'un administrateur ;
    - ▪ télécharger des logiciels sur internet ;
    - ▪ exercer une activité occasionnant une saturation du réseau: téléchargements volumineux ;
    - ▪ échanger des fichiers avec des logiciels de type peer-to-peer (logiciels d'échange et de partage) ;
    - ▪ effectuer des transactions financières.
  - ▸ Fixer la procédure et règles de publication de pages d'information sur les sites internet et intranet de l'établissement (attention à l'hébergement de certains services comme les blogs, les réseaux sociaux, etc…). Rester en conformité avec le RGPD, notamment concernant les lieux d'hébergement et de sauvegarde des données et les conditions générales d'utilisation ;
  - ▸ Chaque utilisateur est informé que l'accès à Internet est soumis à des modalités de filtrage mises en place par les administrateurs du réseau, et que ceux-ci peuvent à tout moment vérifier les connexions effectuées, en cas de besoin.
- ➔ Accès à un réseau Intranet
- ➔ Accès à un Environnement Numérique de Travail (ENT)
- ➔ Accès au Wifi
- ➔ Accès à une messagerie électronique
- ➔ Utilisation de son propre équipement mobile (BYOD[1])
- ➔ AUTRES services

Cet accès a pour objectif exclusif la réalisation d'activités pédagogiques, administratives et éducatives. Tout autre usage est interdit.

Pour accéder à ces matériels et services, l'utilisateur dispose d'un compte d'accès nominatif et individuel. Ce dernier est constitué d'un identifiant et d'un mot de passe strictement personnel et confidentiel. Son usage ne peut en aucun cas être cédé à un tiers à quelque titre que ce soit. L'utilisateur est responsable de leur conservation, s'engage à ne pas les divulguer et à ne pas s'approprier ceux d'un autre utilisateur.

Le CFA de Saône-et-Loire met à disposition des utilisateurs des photocopieurs pour les impressions. L'accès à ces photocopieurs se fait au moyen d'une carte ou d'un badge. Les impressions peuvent être soumises à des quotas. De plus, dans le but d'éviter le gaspillage d'encre, les impressions en Noir & Blanc sont à privilégier.

1 *BYOD = Bring Your Own Device : J'apporte mon propre matériel

Les utilisateurs sont responsables de leurs biens personnels, l'établissement ne pourra être tenu pour responsable en cas de vol, de perte ou de dégradations.

L'utilisation d'équipements personnels connectés aux réseaux sans fil de l'établissement (ordinateur portable, téléphones...) peut être autorisé pour les personnels et les apprenants en faisant la demande aux administrateurs réseaux.

L'autorisation sera soumise aux conditions suivantes:

- Tout utilisateur devra se présenter auprès des administrateurs informatiques avec leur équipement personnel.
- L'utilisateur devra justifier d'un anti-virus performant et à jour. Les administrateurs se donnent le droit de ne pas valider un anti-virus si celui-ci ne parait pas suffisant.
- L'utilisateur devra fournir la ou les adresses MAC du matériel.
- Les utilisateurs autorisent les administrateurs à garder les informations relatives à leur matériel dans un fichier, celui-ci restant confidentiel.
- L'utilisateur doit justifier que son matériel est compatible avec la norme Wi-Fi 802.11 .
- Pour les apprenants, l'accès au réseau Wi-Fi est soumis à des contraintes horaires. Les horaires sont systématiquement affichés sur la page d'accès au réseau Wi-Fi.

Le filtrage des adresses internet s'applique de la même façon sur les postes en réseau sans fil. Les mêmes contrôles que pour les postes fixes pourront être effectués par les administrateurs lorsque les matériels seront présents dans l'établissement.

2.2. Les conditions d'accès aux locaux « TICE »

Les locaux techniques, hébergeant les serveurs sont strictement réservés aux équipes informatiques et cadres de permanence. Les apprenants n'y sont pas autorisés sauf dérogation de ces mêmes personnes.

Les locaux TICE réservés aux apprentissages (salles informatiques, CDI ou autres) sont ouverts aux apprenants sous les conditions suivantes :

- L'ouverture et l'utilisation de ces salles se font sous la responsabilité d'un adulte de l'établissement (formateur, CPE, surveillant...).
- Ces salles sont des espaces dédiés au travail.

3. Les droits et engagements de l'utilisateur

3.1. Le droit d'accès aux ressources informatiques de l'établissement

L'utilisateur bénéficie d'un droit d'accès aux ressources informatiques de l'établissement (ou du centre) selon les modalités précisées dans le paragraphe 2.1.

En cas de poursuites disciplinaires contre l'utilisateur à la suite du non-respect des engagements énoncés dans la présente charte, son droit d'accès peut être suspendu par le directeur de centre concerné dans un premier temps. En cas de sanction disciplinaire et complémentairement à elle, ce droit d'accès pourra être retiré définitivement ou pour une durée déterminée, précisée dans la sanction. S'il est rétabli, ce droit d'accès pourra être limité et réduit.

3.2. Le droit d'accès de l'utilisateur à ses données à caractère personnel

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.

3.3. Les engagements de l'utilisateur

Quel que le soit le support ou matériel utilisé (*), y compris ceux dont il a la propriété (EX : téléphone portable), l'utilisateur est tenu d'en faire un usage qui soit conforme à la fois aux lois et textes en vigueur (3-3-1) mais également aux règles déontologiques ou d'utilisation des matériels et locaux (3-3-2) fixées par cette charte. Toute violation des textes et des règles déontologiques peut donner lieu à des poursuites disciplinaires prévues par le chapitre 6 du règlement intérieur et / ou dépôt de plainte et sans que la liberté d'expression de l'utilisateur puisse être invoquée.

(*) les téléphones portables / messageries électroniques / forums / chats / jeux en ligne / courriers électroniques / réseaux sociaux / site de partage de photographies / blogs / etc…

3.3.1. Les obligations légales de l'utilisateur

* L'utilisateur est tenu de respecter les personnes, qu'elles aient ou pas le statut d'apprenant.

À ce titre et sous peine de sanction, l'utilisation des outils et services numériques :

- ne doit pas conduire à porter atteinte à la vie privée d'un tiers (Art 9 du code civil et 226-1, 226-7 et 226-15 du code pénal), ni à sa dignité (Art 16 du code civil). Le fait d'enregistrer, de capter l'image ou le contenu d'un mail, de filmer et / ou de transmettre au moyen d'un procédé quelconque, sans son consentement, les images et paroles prononcées à titre privé ou confidentiel constitue un acte portant atteinte à la vie privée, à sa dignité et méconnaît son droit à l'image ;

- ne doit pas conduire à tenir des propos injurieux ou diffamatoires, tous deux réprimés par le code pénal (Art R.621-2 du code pénal) et l'article 29 de la loi du 28 juillet 1881 ;

(La diffamation est une allégation ou l'imputation d'un fait qui porte atteinte à l'honneur et à la considération d'une personne)

(Une injure est une parole offensante adressée délibérément à une personne dans le but de la blesser moralement)

- ne doit pas aboutir à un acte de cyberharcèlement ou harcèlement en ligne d'un tiers (Art 222-33-2-2 du code pénal). Le harcèlement scolaire est le fait pour un apprenant ou un groupe d'apprenants de faire subir de manière répétée à un (ou plusieurs) autre(s) apprenant(s) des propos ou des comportements agressifs.

* L'utilisateur est tenu de ne pas consulter de sites, de ne pas transmettre par un moyen électronique des propos, de ne pas fixer, enregistrer, modifier ou diffuser des images à caractère :

- pornographique (Art 227-23 du code pénal),
- homophobe (Art 132-77 du code pénal),
- raciste, antisémite (Art R.625-8-1 du code pénal),
- incitant à la haine raciale (Art R.625-7 du code pénal),
- faisant l'apologie d'acte terroriste ou du crime (Art 421-2-5 du code pénal).

* L'utilisateur notamment majeur est tenu de ne pas transmettre par un moyen électronique des propos, de ne pas fixer, enregistrer, modifier ou diffuser des images mettant en péril un mineur notamment en l'incitant :

- à l'usage illicite de stupéfiants (Art 227-18 du code pénal),
- à la consommation excessive de boissons alcooliques (Art 227-19 du code pénal),
- à la commission de crimes ou de délits (Art 227-21 du code pénal),
- au suicide (Art 223-13 du code pénal),
- à se mettre en danger (Arts 223-1 et 223-2 du code pénal)

* L'utilisateur est tenu de respecter le droit d'auteur des œuvres littéraires, musicales, photographiques ou audiovisuelles mises en ligne, et d'une manière générale, le respect du code de la propriété intellectuelle.

Le droit de publication reconnu à l'utilisateur quelles que soient les modalités de sa mise en œuvre (vidéo, blog, journal en ligne, partage de travaux scolaires, etc…) implique un respect du droit d'auteur reconnu par le code de la propriété intellectuelle à deux titres :

- D'une part, l'utilisateur peut être considéré comme « auteur » si sa « production » a un caractère original et ne constitue pas un « travail scolaire ». Cette qualité lui confère des droits patrimoniaux sur ses productions mises en ligne. L'exploitation et la réutilisation de ces productions nécessitent son autorisation préalable et exigent que les ré-utilisateurs précisent les sources du document.
- D'autre part, l'utilisateur lorsqu'il n'est pas sous la direction et l'autorité d'un formateur pour réaliser sa production, doit se conformer à la réglementation sur le droit d'auteur (autorisation et citation des sources) dès lors que le document utilisé pour la réalisation de sa production est considéré comme une œuvre protégée par le code la propriété intellectuelle.

La méconnaissance de ces règles est une infraction (délit de contrefaçon) sanctionnée par l'article L.353-3 du code de la propriété intellectuelle.

3.3.2. Les engagements de l'utilisateur en cas d'utilisation des matériels et locaux

Les services offerts par le réseau (stockage des données, accès intranet et internet) sont destinés à un usage pédagogique et éducatif, dans le cadre de la vie de l'établissement, et leur utilisation doit s'effectuer dans le respect des textes législatifs et réglementaires en vigueur.

Chaque utilisateur est responsable de l'utilisation qu'il fait de ces services et s'engage à ne pas effectuer d'opérations pouvant nuire au fonctionnement du réseau.

Chaque utilisateur s'engage à informer le formateur ou les personnes responsables de toute anomalie ou de tout dysfonctionnement constaté avant de quitter son poste.

Chaque utilisateur s'engage à informer l'établissement de toute perte, anomalie ou tentative de violation de ses codes d'accès personnels

Entre autres, l'utilisateur ne doit en aucun cas :

- Masquer sa propre identité ou s'approprier le mot de passe du compte d'autrui ;
- Obtenir le mot de passe d'un autre utilisateur ;
- Altérer les données ou accéder à des informations appartenant à d'autres utilisateurs du réseau sans leur autorisation ;
- Porter atteinte à l'intégrité d'un autre utilisateur, à sa personnalité ou sa sensibilité, notamment par l'intermédiaire de messages, textes ou images provocants ;
- Procéder à l'installation d'un logiciel sur un ordinateur du réseau et le rendre accessible sans accord préalable d'un administrateur ;
- Télécharger des logiciels sur internet ;
- Contourner les restrictions d'utilisation d'un logiciel ;
- Interrompre le fonctionnement normal du réseau ou d'un des systèmes connectés au réseau ;
- Exercer une activité occasionnant une saturation du réseau : téléchargements volumineux ;
- Modifier sans autorisation la configuration des machines (déconnexion de périphériques, changement de cartouches, ...) ;
- Stocker des fichiers dont il ne détient pas les droits dans son espace personnel ;
- Ne pas débrancher du réseau les matériels mis à disposition sauf en ce qui concerne les matériels « portables », sous les conditions édictées par le règlement d'utilisation ;
- Ne pas brancher d'ordinateur personnel sur le réseau ;
- Échanger des fichiers avec des logiciels de type peer-to-peer (logiciels d'échange et de partage) ;
- Stocker des fichiers audio et vidéo ;
- Effectuer des transactions financières.

4. Les engagements de l'établissement

L'établissement fait bénéficier l'Utilisateur d'un accès aux ressources et services multimédias

4.1. Le respect de la loi

L'établissement s'oblige à respecter toutes les règles protectrices des intérêts des tiers et de l'ordre public et notamment à informer promptement les autorités publiques des activités illicites qu'il pourrait constater à l'occasion de l'utilisation de ses services.

4.2. La disponibilité du service

L'établissement s'oblige à donner un accès facile, direct et permanent, pour les destinataires de ses services.

L'établissement s'engage à informer l'utilisateur de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner, et à leur proposer au moins un de ces moyens.

4.3. La protection des utilisateurs

L'établissement et l'équipe pédagogique se doivent de protéger les utilisateurs mineurs en les préparant, en les conseillant, en les assistant dans leur utilisation de l'internet et des réseaux numériques.

Il appartient à l'établissement et à l'équipe pédagogique de veiller, au cas par cas, à une organisation de ces activités offrant de bonnes conditions de sécurité. La mise en place de ces mécanismes de protection doit se faire de manière adaptée aux très diverses situations d'apprentissage, selon que l'utilisation s'effectue dans la salle de formation, en centre de documentation ou en salle multimédia, qu'il nécessite le parcours d'un large éventail de sites ou au contraire la restriction à quelques pages web liées à l'activité du jour ou de l'heure.

4.4. La protection des données à caractère personnel de l'utilisateur

L'établissement s'engage à donner suite aux demandes de l'utilisateur pour faire valoir ses droits sur ses données personnelles conformément aux dispositions du 3-2 de la présente charte.

4.5. L'information en cas de contrôles techniques

L'établissement informe l'utilisateur que les différents dispositifs du système d'information, liés à la gestion de la sécurité et à la recherche de pannes et incidents, enregistrent des informations le concernant.

L'établissement informe l'utilisateur qu'il peut procéder à des contrôles à posteriori des sites internet visités et des durées correspondantes.

5. Les modalités de la sensibilisation et de l'éducation aux outils et services numériques

La charte décline l'organisation mise en place localement et éventuellement régionalement pour permettre aux utilisateurs (en particulier les nouveaux) de s'autoréguler sur internet et être sensibilisés aux risques et aux enjeux.

6. Les contrôles techniques et sanctions

Des contrôles techniques peuvent être effectués par l'établissement :

→ **soit dans un souci de protection des apprenants et notamment des mineurs ;**

L'établissement se réserve la possibilité de procéder à un contrôle des sites visités par les apprenants afin d'éviter l'accès par ces derniers à des sites illicites ou requérant l'âge de la majorité, notamment par lecture des journaux d'activité du service d'accès au réseau.

→ **soit dans un souci de sécurité du réseau et/ou des ressources informatiques ;**

Pour des nécessités de maintenance et de gestion technique, l'utilisation des services et notamment des ressources matérielles et logicielles ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable et notamment dans le respect des règles relatives à la protection de la vie privée et au respect des communications privées. L'établissement se réserve, dans ce cadre, le droit de recueillir et de conserver les informations nécessaires à la bonne marche du système.

L'utilisateur est informé que les différents dispositifs du système d'information, liés à la gestion de la sécurité et à la recherche de pannes et incidents, enregistrent des informations le concernant.

L'utilisateur est informé que l'établissement se réserve le droit de procéder à des contrôles à posteriori des sites internet visités et des durées correspondantes.

Ces dispositifs permettant l'identification d'utilisations contraires aux principes et dispositions de la présente charte, l'administrateur du réseau pourra dans cette hypothèse être amené à signaler ces informations au directeur de l'établissement et au directeur de centre concerné. Ces signalements peuvent donner lieu à des poursuites disciplinaires de l'apprenant dans le cadre de la procédure prévue à cet effet par le règlement intérieur et / ou à des signalements aux autorités judiciaires si les faits constatés sont constitutifs d'infractions pénales.

Les données personnelles collectées sont détruites dans un délai d'un an. Les personnels chargés des opérations de contrôles sont soumis au secret professionnel.

En cas de faute disciplinaire ou d'infraction commise par un utilisateur qui serait liée à l'usage des outils et services numériques, le directeur peut limiter ou retirer ses autorisations d'accès de manière temporaire ou définitive.

En cas d'urgence, les administrateurs informatiques pourront être amenés à prendre toutes dispositions propres à assurer l'intégrité et la sécurité des systèmes et des utilisateurs (fermeture de compte….).

Les administrateurs peuvent être amenés à interrompre le fonctionnement du réseau, complet ou partiel à des fins de maintenance, les utilisateurs en seront préalablement informés.

7. Les dispositions finales

La charte est intégrée sous forme d'annexe au règlement intérieur de l'établissement. Elle est diffusée selon les modalités suivantes :

- Affichée au CDI
- Affichée sur la page d'accueil lors de la connexion au WIFI pédagogique
- Téléchargeable sur le site intranet de l'établissement
- Jointe aux dossiers d'inscription des apprenants

Il est convenu que chaque utilisateur ou ses représentants légaux s'il est mineur atteste(nt) en avoir pris connaissance selon les mêmes modalités que les autres dispositions du règlement intérieur. La charte peut être modifiée et révisée à l'issue ou le cas échéant en cours d'année de formation.

Je déclare avoir pris connaissance de la charte et en comprendre les règles

Date :

Signature :

ANNEXE 1 : GLOSSAIRE DES TERMES TECHNIQUES

S'Il appartient à l'établissement de convenir de la bonne définition des termes techniques employés dans la charte, les termes suivants ont une définition légale :

Administrateur : un administrateur est une personne chargée de la maintenance et du suivi d'un système informatique.

Cyber harcèlement : La Commission nationale de l'informatique et des libertés (CNIL) identifie le cyber harcèlement comme étant « le fait de recevoir des messages répétés dont le contenu est teinté de menaces, d'insultes ou de chantage. Les auteurs de ces messages peuvent aussi demander de l'argent pour arrêter, exiger une rencontre ou demander des informations privées ».

Données personnelles : Une donnée personnelle (ou donnée à caractère personnel) est une information relative à une personne physique identifiée ou qui peut être identifiée, directement (Ex : nom prénom) ou indirectement (Ex : numéro téléphone, menu cantine particulier, etc…) par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

Données sensibles : Ce sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. Le RGPD interdit de recueillir ou d'utiliser ces données, sauf dans certains cas.

EIM : Le terme "équipement individuel mobile" désigne les ordinateurs portables, les tablettes, les téléphones portables et les liseuses. Ces équipements sont individuels car ils permettent l'accès d'un seul utilisateur, apprenant ou formateur, aux ressources pédagogiques et mobiles car ils sont utilisés dans les situations d'usages pédagogiques nomades dans la salle de formation et en dehors de celle-ci. Leur déploiement est régi par le CARMO pour « Cadre de référence pour l'Accès aux Ressources pédagogiques via un équipement Mobile », ce référentiel regroupe toutes les préconisations et recommandations sur le déploiement des Équipements individuels MObiles dans les établissements d'enseignement et de formation.

ENT : Un Espace Numérique de Travail (ENT) est un portail internet éducatif permettant à chaque membre de la communauté éducative d'un établissement de formation, d'accéder, via un point d'entrée unique et sécurisé, à un bouquet de services numériques en relation avec ses activités. Le ministère de l'éducation nationale publie le schéma directeur des espaces numériques de travail (SDET) afin de définir l'architecture de référence ainsi que les services attendus dans les espaces numériques de travail et de formaliser les préconisations organisationnelles, fonctionnelles et techniques.

CGU : conditions générales d'utilisation déterminent les règles d'accès à un service informatique, (logiciel, site web, plateforme…)

Internet : réseau mondial associant des ressources de télécommunications et des matériels informatiques et numériques (ordinateurs, serveurs, smartphones…) destiné à l'échange de messages électroniques, d'informations multimédia et de fichiers.

Intranet : réseau de télécommunication et de téléinformatique destiné à l'usage exclusif d'un organisme (ici un CFA) utilisant les mêmes protocoles et techniques que l'internet.

MAC (adresse) : identifiant physique stocké dans une carte réseau ou une interface réseau similaire. À moins qu'elle n'ait été modifiée par l'utilisateur, elle est unique au monde. Toutes les cartes réseau ont une adresse MAC, même celles contenues dans les PC et autres appareils connectés (tablette tactile, smartphone, consoles de jeux…).

Messagerie électronique : service permettant aux utilisateurs habilités de saisir, envoyer ou consulter en différé des courriers électroniques ou courriels.

Mot de passe fort ou robuste : mot de plus de douze caractères ou phrase qui contient au moins un nombre, une majuscule, un signe de ponctuation ou un caractère spécial (dollar, dièse, ...)

Registre des activités de traitement : Le registre est prévu par l'article 30 du RGPD. Il participe à la documentation de la conformité. C'est un document de recensement et d'analyse, il doit refléter la réalité de vos traitements de données personnelles et vous permet d'identifier précisément :

- les parties prenantes (représentant, sous-traitants, co-responsables, etc.) qui interviennent dans le traitement des données,
- les catégories de données traitées,
- à quoi servent ces données (ce que vous en faites), qui accède aux données et à qui elles sont communiquées,
- combien de temps vous les conservez,
- comment elles sont sécurisées.

Ressource pédagogique numérique : la définition donnée par le standard LOM (Learning Object Metadata) précise qu'une ressource pédagogique numérique est une entité numérique utilisée dans un processus d'enseignement, de formation ou d'apprentissage.

RGPD : Le Règlement Général sur la Protection des Données (RGPD) est le nouveau cadre juridique de l'Union européenne qui gouverne la collecte et le traitement des données à caractère personnel des utilisateurs. Il est entré en vigueur le 25 mai 2018.

Utilisateur : en informatique, le terme utilisateur est employé pour désigner une personne qui utilise un système informatisé mais qui n'est pas nécessairement informaticien.

Wifi (Wireless fidelity): norme internationale d'accès sans fil à internet par radiocommunication. Le ministère de l'éducation nationale publie un **référentiel Wi-Fi** qui apporte aux différents acteurs du numérique éducatif les éléments à prendre en compte lors de la mise en place du Wi-Fi en établissement et école, afin de les aider à obtenir une infrastructure fiable et adaptée aux usages.

ANNEXE 2 : RÉFÉRENCES RÉGLEMENTAIRES

- **La loi n°88-19 du 5 janvier 1988** modifiée par **Loi n°2004-575 du 21 juin 2004** relative à la fraude informatique a créé des infractions spécifiques en la matière, reprises par **les articles 323-1 à 323-7** du code pénal. Ainsi, il est notamment disposé :

  - **Art 323-1**

    "Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende.

    Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende".

  - **Art 323-2**

    "Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 € d'amende".

  - **Art 323-3**

    "Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 € d'amende".

  - **Art 323-3-1**

    "Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée".

  - **Art 323-4**

    "La participation à un groupement formé ou à une entente établie en vue de la préparation caractérisée par un ou plusieurs faits matériels, d'une ou plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée".

  - **Art 323-5**

    "Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

    1. L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de **l'article 131-26** ;
    2. L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;
    3. La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;
    4. La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
    5. L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;
    6. L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;
    7. L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par **l'article 131-35**".

- **Art 323-7**

  "La tentative des délits prévus par les articles 323-1 à 323-3-1 est punies des mêmes peines".

- **La loi n°78-17 du 6 janvier 1978** (consolidée au 22 décembre 2007): relative à l'informatique, aux fichiers et aux libertés (consolidée au 22 décembre 2007).
- **La loi n°85-660 du 3 juillet 1985** (consolidée au 01 mars 2006): relative aux droits d'auteur, a étendu aux logiciels en tant qu'œuvres de l'esprit, la protection prévue par la loi n°57-298 du 11 mars 1957 sur la propriété littéraire et artistique (cf. notamment article L 335-2 du code de la propriété intellectuelle qui prévoit le délit de contrefaçon des œuvres protégées).
- **La loi n° 2006-961 du 1er août 2006** relative au droit d'auteur et aux droits voisins dans la société de l'information (DADVSI).
- **Loi N°86-1067 du 30 septembre 1986** (consolidée au 07 mars 2007): Relative à la liberté de communication
- **Loi N°89-486 du 10 juillet 1989** relative à l'orientation sur l'éducation