

CHARTRE D'USAGE DES OUTILS ET SERVICES NUMERIQUES PAR LES APPRENANTS DE L'ETABLISSEMENT D'ENSEIGNEMENT DE L'EPLEFPA DES LANDES

Table des matières

PRÉAMBULE.....	2
1. Le périmètre de la charte.....	2
1-1. Les utilisateurs concernés.....	2
1-2. Les lieux et services concernés.....	2
2. Les règles relatives à l'utilisation des locaux et des ressources informatiques.....	2
2-1. Conditions d'accès aux matériels et services informatiques.....	3
2-2. Les conditions d'accès aux locaux « TICE ».....	4
3. Les droits et engagements de l'utilisateur.....	4
3-1. Le droit d'accès aux ressources informatiques de l'établissement.....	4
3-2. Le droit d'accès de l'utilisateur à ses données à caractère personnel.....	5
3-3. Les engagements de l'utilisateur :.....	5
3-3-1. Les obligations légales de l'utilisateur.....	5
3-3-2. Les engagements de l'utilisateur en cas d'utilisation des matériels et locaux.....	7
4. Les engagements de l'établissement.....	7
4-1. Le respect de la loi.....	7
4-2. La disponibilité du service.....	7
4-3. La protection des utilisateurs.....	8
4-4. La protection des données à caractère personnel de l'utilisateur.....	8
4-5. L'information en cas de contrôles techniques.....	8
5. Les modalités de la sensibilisation et de l'éducation aux outils et services numériques.....	8
6. Les contrôles techniques et sanctions.....	8
7. Les dispositions finales.....	9
ANNEXE 1 : Glossaire des termes techniques.....	10

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 (élèves, étudiants, apprentis et stagiaires) 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 de l'établissement.

Salles de classes, salle de cours d'informatique, salles techniques, internats, exploitations agricoles

2- à l'ensemble des services et outils numériques mis à disposition de l'utilisateur.

Les ressources informatiques sont constituées de l'ensemble des ordinateurs de l'EPLEFPA, des serveurs ainsi que des matériels audiovisuels, des imprimantes, des périphériques, des logiciels et des accès à Internet.

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 scolaires 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. ...)

Les salles de cours informatique ainsi que le centre de ressources (CDR) sont accessibles uniquement pour les cours, ainsi que pour les études.

Chaque utilisateur dispose d'un compte informatique individuel. Il dispose d'un code personnel, ainsi que d'un espace disque personnel, lui permettant de stocker ses travaux.

La connexion au réseau est obligatoire, elle permet de s'authentifier sur le serveur et ainsi de bénéficier des services d'anti-virus, accès Internet, imprimantes réseau, et des différents espaces de stockage communs.

Chaque utilisateur est responsable de l'utilisation de son compte et du secret de son mot de passe.

L'utilisateur préviendra le service informatique si son mot de passe ne lui permet plus de se connecter ou s'il soupçonne que son compte est utilisé par une autre personne.

Chaque utilisateur est responsable de la sécurité de ses propres fichiers. L'EPLEFPA décline toute responsabilité en cas de dommage ou perte de données découlant directement ou indirectement de l'utilisation de ses ressources informatiques. L'EPLEFPA s'efforce toutefois, dans la mesure de ses moyens, de prendre les dispositions et décisions nécessaires pour assurer la sécurité et le bon fonctionnement de ses ressources informatiques. Il peut en particulier :

- surveiller les débits ;
- exercer une vigilance sur l'activité des comptes utilisateurs ;
- retirer le droit d'accès d'un utilisateur, après avoir invité celui-ci à présenter ses observations ;
- limiter voire effacer les fichiers qui prennent une place excessive. La décision d'effacer un fichier ne peut toutefois être prise qu'après information de l'utilisateur concerné. Il peut toutefois être dérogé à cette obligation d'information préalable en cas d'urgence.

Les données du réseau sont sauvegardées au moins 1 fois par semaine sur un espace dédié et 4 semaines de sauvegardes sont conservées.

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 :**

Le réseau internet de l'EPLEFPA des Landes est relié au réseau régional GREPA (système de réseau Aquitaine) grâce auquel il est possible d'accéder à RENATER (Réseau National pour la Technologie, l'Enseignement et la Recherche) et à l'Internet.

L'utilisation d'Internet est réservée à des fins de formation. Le service informatique peut suivre les connexions individuelles (adresses des sites consultés). Un filtrage de sites (liste noire éditée par l'académie de Toulouse) a été mis en place et est régulièrement mis à jour.

En cas d'utilisation sur des sites non conformes (sites à caractères pornographiques, pédophiles, xénophobes, racistes, terroristes etc.), l'accès au compte Internet pourra être supprimé, des poursuites pénales pourraient être engagées par ailleurs.

- **Accès à un Environnement Numérique de Travail (ENT) comprenant :**

- Un accès aux données de vie scolaire Pronote (notes, cahier de texte, absences, etc...);
- Un service de diffusion d'informations et de mise en ligne de contenus (publication web);
- Un service d'accès à des ressources pédagogiques numériques;
- Des services de communication électronique (messagerie instantanée, forums de discussion);
- Un service de téléchargement et de stockage de contenus.

- **Accès au Wifi**

La surveillance et le filtrage des accès au WIFI est le même que celui mis en place sur réseau filaire (filtrage des sites internet, logs de connexions)

Les conditions d'utilisations sont les mêmes que pour l'accès au réseau filaire.

Pour les internats, un portail captif permet l'authentification de l'utilisateur.

Règles de protection du matériel personnel

- Les apprenants doivent impérativement prendre des précautions pour éviter l'infection (virus) de leur ordinateur et ceux de leurs collègues.
- Mettre à jour régulièrement les correctifs du système d'exploitation.
- Installer un anti-virus et le mettre à jour régulièrement.

L'utilisation du réseau sans-fil que l'établissement met à disposition, implique la pleine acceptation des règles ci-dessus. En cas de non-respect de ces règles, l'établissement se réserve le droit de désactiver les accès.

L'utilisateur reconnaît être dans un établissement public. Il s'engage à utiliser son matériel informatique, (portable, Smartphone, tablette,..) et ce service, d'une manière conforme à la loi et à la net étiquette (charte de bonne conduite sur internet).

- **Utilisation de son propre équipement mobile (BYOD)**

Le matériel dit « matériel personnel » concerne les ordinateurs fixes ou portables, téléphones, smartphones, tablettes, imprimantes, etc.

L'EPLEFPA des Landes n'est pas responsable du matériel des élèves, apprentis, stagiaires et du personnel. Tout dysfonctionnement ou casse sur les matériels personnels relève de la responsabilité de son propriétaire ou du responsable légal pour les élèves mineurs.

- **Autres services**

L'usage des ordinateurs portables et matériels empruntés est soumis, comme tous les postes informatiques de l'établissement, au règlement de la charte informatique de l'EPL de Dax.

Une fiche de prêt est signée par l'emprunteur et le prêteur du matériel.

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 voir paragraphe 2.

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.

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 complémentarément 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 paragraphe 6 de cette charte et dans le du règlement intérieur .

(*) *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.**

A 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 cyber harcèlement 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 enseignant 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 de 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

Chaque utilisateur s'engage à :

- Respecter les consignes d'utilisation afin de garantir le bon fonctionnement des outils informatiques et multimédia.

Un utilisateur ne doit jamais quitter un poste de travail sans se déconnecter.

Respecter les autres, ne pas accéder, s'approprier, altérer ou détruire des ressources appartenant à d'autres utilisateurs sans leur autorisation.

Respecter le matériel

- La réservation au service informatique de tout matériel numérique est obligatoire avant de l'emprunter pour son utilisation. A partir de l'intranet il est possible de consulter l'état des réservations. Tous les matériels empruntés (portables, etc.) devront être rendus avant chaque vacance scolaire.
- Prendre soin du matériel et prévenir un informaticien de toute anomalie constatée.
- Ne pas installer les logiciels n'appartenant pas à l'établissement.
- **Il est interdit d'amener des boissons ou de la nourriture dans les salles informatiques.**
- Respect des droits d'auteur

Dans le respect du droit d'auteur, la publication ou la distribution des documents ou logiciels téléchargés doit se faire avec la permission de leur propriétaire. Les utilisateurs s'engagent à citer les sources d'où proviennent leurs documents.

Toute personne contrevenant à ces règles sera sanctionnée.

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 classe, 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

En classe, les premières séances d'accompagnement personnalisé sont prévues pour informer les élèves et apprenants de leurs droits et devoirs à l'utilisation des outils et services numériques mis à leur disposition.

Les programmes d'informatique permettent de travailler sur les usages en classe.

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.

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.

- Sur le site internet de l'EPLFPA des Landes : www.formagri40.
- Sur l'ENT Lycée connecté , YPAREO, G-Suite, Pronote et l'intranet de l'établissement
- Mise à disposition-au CDI et dans les salles informatiques

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 scolaire.

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 ».
- **BYOD** : abréviation de l'anglais « **bring your own device** », en français, PAP pour « prenez vos appareils personnels » [1] ou AVEC pour « apportez votre équipement personnel de communication » [2], est une pratique qui consiste à utiliser ses équipements personnels (smartphone, ordinateur portable, tablette électronique) dans un contexte professionnel.
- **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, élève ou enseignant, aux ressources pédagogiques et mobiles car ils sont utilisés dans les situations d'usages pédagogiques nomades dans la classe et hors la classe. 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 Equipements individuels MObiles dans les écoles et collèges.
- **ENT** : Un espace numérique de travail (ENT) est un portail internet éducatif permettant à chaque membre de la communauté éducative d'un établissement scolaire, 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.

- **GAR** : Le Gestionnaire d'Accès aux Ressources (GAR) est un traitement de données à caractère personnel relevant du Ministère de l'Éducation nationale et dont l'opérateur est RENATER. Il a pour objet de permettre l'accès des élèves et des enseignants à leurs ressources numériques et services associés via un espace numérique de travail (ENT) ou un équipement mobile.
- **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, smartphone...) 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 EPLEFPA) utilisant les mêmes protocoles et techniques que l'internet.
- **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.
- **SI** : Systeme d'information
- **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.