MINISTÈRE
DE L'AGRICULTURE
ET DE LA SOUVERAINETÉ
ALIMENTAIRE

Liberté
Égalité
Fraternité

NumEA
Numérique Éducatif
de l'Enseignement Agricole

Guide des principales règles en matière d'USAGE DU NUMÉRIQUE

dans les établissements scolaires de l'enseignement agricole

https://chlorofil.fr/numerique/plan-2018-2020/suivi/reglementaire

Table des matières

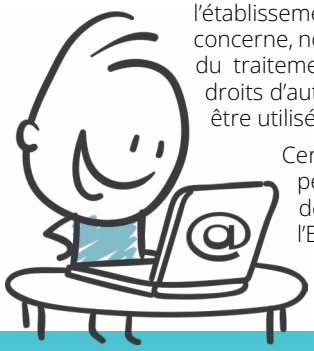
PRÉAMBULE

La fourniture des services numériques fait partie intégrante de la mission de service public de l'éducation. Elle répond à un double objectif, à la fois pédagogique et éducatif. Cependant, l'usage des outils et services numériques peut présenter des risques juridiques, voire judiciaires dans certains cas. C'est pourquoi il est important d'informer et de sensibiliser les directeurs d'établissement offrant ces services, et plus largement l'ensemble de la communauté éducative, utilisatrice des outils et services numériques qui leur sont accessibles, **aux règles et devoirs associés à l'utilisation de ces derniers**.

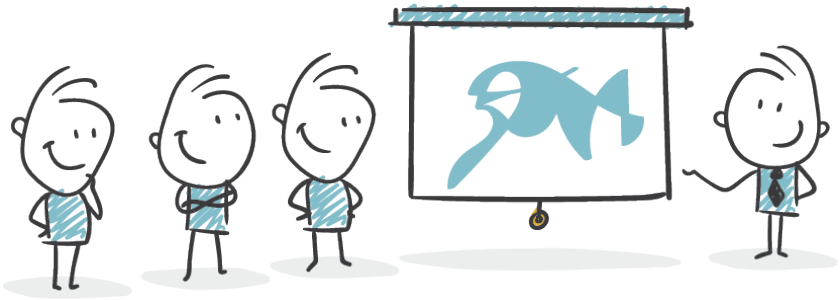
Le présent guide constitue, de manière non exhaustive, une ressource à laquelle vous pouvez vous référer pour comprendre le sens des règles qui encadrent l'utilisation des ressources numériques. Ces dernières sont de deux ordres :

- ressources mises à votre disposition par l'établissement, ce dernier étant de fait soumis à des engagements de service et de sécurité,
- ressources que vous aurez librement choisies et qui nécessitent une attention plus particulière en matière de respect du droit.

Ce guide se veut ainsi un condensé des droits et obligations que l'établissement et l'utilisateur doivent respecter, chacun en ce qui le concerne, notamment en matière de droits des personnes au regard du traitement des données personnelles ainsi qu'en matière de droits d'auteur, au regard des ressources numériques qui peuvent être utilisées pour la préparation de séquences d'apprentissage.



Certaines règles de bonne pratique, ainsi que les fiches pédagogiques auxquelles il est fait référence, ont été tirées des ressources de la CNIL, et du guide de droit d'auteur de l'ENSSIB qui nous ont donné leur accord pour utiliser leurs ressources dans le cadre de ce guide. Ce préambule permet de les remercier pour cette autorisation.



1

DESCRIPTION DES SERVICES ET OUTILS NUMÉRIQUES UTILISABLES PAR LES PERSONNELS

1.1 SERVICES ET OUTILS MIS À DISPOSITION PAR LES ÉTABLISSEMENTS

L'établissement offre au personnel, ci-après également dénommé l'utilisateur, des outils et services numériques le plus souvent au sein d'un espace numérique de travail (ENT). À titre d'exemple, cet ENT comprend : des services pédagogiques (cahier de texte numérique, espaces de travail et de stockage communs aux élèves et aux enseignants, accès aux ressources numériques, outils collaboratifs, blogs, forums, classes virtuelles, etc.), des services d'accompagnement de la vie scolaire (notes, absences, emplois du temps, agendas, etc.) et des services de communication (messagerie, informations des personnels et des familles, visioconférence, etc.). L'utilisateur bénéficie d'un accès aux services proposés par l'établissement, avec éventuellement des restrictions visant à garantir la sécurité du réseau de l'établissement ainsi que le respect de toutes les règles protectrices des intérêts des tiers et de l'ordre public. Il bénéficie également des outils mis à disposition par la Direction du Numérique Éducatif (DNE) du ministère chargé de l'éducation nationale https://apps.education.fr/.

Cet ensemble intégré de services numériques met en œuvre les moyens suivants : matériel informatique (ordinateurs, serveurs), des moyens audiovisuels (caméra, TV), des moyens d'impression, une connexion au réseau informatique de l'établissement (intranet), la possibilité de navigation sur le réseau Internet (un service de recherche sur le Web)...

Les solutions proposées par l'établissement offrent de nombreux avantages notamment en termes de sécurisation du réseau de l'établissement et en termes de contrôle des données personnelles, les applications ayant été choisies en conformité avec le Règlement Général sur la Protection des Données (RGPD). Cependant, même un établissement qui revendique un fort taux d'équipements numériques ne sera jamais en mesure de répondre à tous les besoins des enseignants et des formateurs. C'est pourquoi il est plus que tentant d'utiliser des outils personnels (ordinateurs personnels, logiciels ou autres ressources numériques téléchargées ou utilisées en ligne). Si cela est absolument nécessaire, il convient de configurer un compte utilisateur qui ne servira que pour se connecter au domaine de l'établissement, vous pourrez pour cela faire appel au professeur TIM (technologies de l'informatique et du multimédia) ou au Technicien formation recherche IBA (informatique, bureautique, audiovisuel) recherche de votre établissement, après validation de votre chef(fe) d'établissement.

1.2 OUTILS ET SERVICE PERSONNELS OU ACCESSIBLES EN LIGNE PAR L'UTILISATEUR

Les éditeurs d'outils numériques regorgent d'outils performants, tous plus intéressants les uns que les autres par rapport à l'objectif visé par le formateur ou l'enseignant. Malgré la souplesse, l'attractivité et la performance que ces outils et services apportent à l'utilisateur, ces accès ne se font pas sans contrepartie, notamment en termes de traces et d'informations personnelles que nous laissons sur Internet. Ces informations permettent, par recoupement entre plusieurs sources, d'identifier un individu, notamment par le biais des cookies, adresses IP, comptes Google…

L'inspection de l'enseignement agricole préconise de ne pas utiliser des solutions numériques dont les serveurs sont hébergés dans des lieux n'appliquant pas le RGPD (USA, Russie, Chine…).

Les pays de l'Union européenne offrent des garanties de sécurité, du fait de leur engagement à appliquer le RGPD. Malgré cela, il convient d'être vigilant à la protection des données personnelles qui pourraient être utilisées à des fins commerciales par certains sites web.

EXEMPLES

1- LES BONS RÉFLEXES À AVOIR

- Utiliser préférentiellement les outils du socle interministériel de logiciels libres (SILL) https://www.numerique.gouv.fr/actualites/decouvrez-le-socle-interministeriel-des-logiciels-libres-sill-2019/.
- Toujours lire les Conditions Générales d'Utilisation (CGU) avant d'installer, de cocher ou d'autoriser une application.

Vous pourrez vérifier, à l'aide d'un traceur, par où transitent et où sont hébergées les données (commande MS-Dos tracert et utilisation d'outil type https://www.my-ip-finder.fr/ ou http://www.infowebmaster.fr/outils/localiser-site-web.php…).

- Toujours autoriser l'accès au minimum de données, et, pour cela, bien paramétrer votre navigateur (notamment pour les cookies).
- Installer un système antivirus de cyber-sécurité complet (anti-maliciel, anti-ramsonware, anti-spyware, anti-hameçonnage, protection de webcam et micro, gestionnaire de mots de passe, pare-feu, VPN, contrôles parentaux, protection réseaux sociaux, anti-traçage, antivol par cryptage, géolocalisation, anti-fraude…) et le maintenir à jour (ex. : Bitdefender, BullGuard, Kaspersky, Mc Afee, Norton, Panda, Trend…).
- Utiliser un VPN dès que l'on se connecte à Internet en dehors des zones de confiance (restaurant, hôtel, hotspot Wifi…).

DE BONS USAGES

— Bien distinguer usage professionnel et usage privé.

— Se connecter en administrateur local ou de domaine le moins souvent possible.

— Utiliser des mots de passe forts et les changer régulièrement.

— Effectuer des sauvegardes régulières de ses données sur un support amovible ou un cloud sécurisé, hébergé dans l'Union européenne.

— Crypter ses données et fichiers lorsqu'ils sont sensibles ou confidentiels.

2- UTILISER AU MAXIMUM, LES OUTILS DES ÉDITEURS SCOLAIRES

Les éditeurs scolaires intègrent les avancées scientifiques, technologiques et sociétales dans les ressources qu'ils éditent ; **une licence** permet de se prémunir contre des fuites de données.

— Utiliser au maximum les outils hébergés dans l'ENT.

— Accéder aux outils préconisés par la direction du numérique éducatif, disponibles sur Apps.education : https://apps.education.fr/ qui permettent d'utiliser des outils collaboratifs validés.

Pour des outils non disponibles, ayez le réflexe de demander conseil aux professeurs de TIM ou d'informatique de votre établissement qui possèdent certainement déjà des licences sur de nombreux matériels et qui vous permettront de choisir avec soin l'outil approprié.

2

ENGAGEMENTS DE L'UTILISATEUR

La quantité et la facilité de circulation des informations et des contenus sur Internet ne doivent pas faire oublier la nécessité de respecter la législation en vigueur. Ainsi, le rappel, non exhaustif, de certaines règles de droit relatives à l'utilisation des outils numériques proposés par un établissement scolaire, vise le triple objectif de sensibiliser l'utilisateur à leur existence, à leur respect, ainsi qu'à la prévention d'actes illicites. Les utilisateurs sont donc tenus de respecter entre autres :

- **le droit des personnes**, en ne portant pas atteinte à la vie privée d'autrui, en veillant à ne pas diffuser de propos injurieux, diffamatoires ou des rumeurs (parties 2.1 et 2.2),
- **le droit d'auteur et de la propriété intellectuelle** (parties 2.3 à 2.5),
- **l'ordre public** en veillant à ne pas diffuser des propos discriminatoires, ou faisant l'apologie de crimes ou de délits,
- **l'intégrité des ressources informatiques** en veillant à ne pas effectuer des opérations pouvant nuire au fonctionnement des plateformes numériques ou du réseau.

L'utilisateur s'engage à informer la direction d'établissement de l'existence de contenus ou comportements illicites dont il aurait connaissance, ainsi que de toute perte, tentative de violation ou autre anomalie relative à l'utilisation de ses codes d'accès personnels.

2.1 LE DROIT À LA PROTECTION DES DONNÉES PERSONNELLES

Il s'agit d'un droit fondamental consacré par l'article 8 de la Charte des droits fondamentaux de l'Union européenne et le Règlement Général sur la Protection des Données (RGPD) adopté par le Parlement européen le 27 avril 2016.

Le RGPD est entré en application dans les États membres de l'Union européenne le 25 mai 2018. Il s'agit, au niveau européen, du principal texte de référence, intégré dans la législation française par la loi informatique et libertés[1]. Ces textes ont pour objectif d'assurer à chacun une meilleure maîtrise de ses données personnelles en renforçant ses droits sur celles-ci, comme, par exemple, le droit à l'effacement. Concrètement, le règlement encadre les conditions dans lesquelles les données personnelles peuvent être traitées, c'est-à-dire recueillies, enregistrées, conservées, communiquées ou même seulement consultées. Le RGPD prévoit, à cet effet, que les règles soient respectées par tous les acteurs qui traitent ces données (entreprises, administrations, écoles, responsables de sites, de réseaux sociaux, associations, etc.) et les oblige à être transparents, c'est-à-dire à **informer les personnes auprès desquelles sont recueillies les données, de l'utilisation qui en sera faite.**

1- Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés

MAIS AU FAIT, C'EST QUOI UNE DONNÉE PERSONNELLE ?

D'après la CNIL, « Est considéré comme donnée personnelle, tout renseignement consigné ayant trait à une personne, qui peut ainsi être identifiée. En raison de la nature des données qui concernent des personnes physiques, ces dernières doivent en conserver la maîtrise. »

Une personne physique peut ainsi être identifiée soit **directement** (exemple : nom et prénom) soit **indirectement** (exemple : par un numéro de téléphone ou de plaque d'immatriculation, un identifiant tel que l'INE, une adresse postale ou un courriel, mais aussi la voix ou l'image).

L'identification d'une personne physique peut être réalisée :

- à partir **d'une seule donnée** (exemple : nom),
- à partir **du croisement d'un ensemble de données** (exemple : une femme vivant à telle adresse, née tel jour et membre dans telle association).

Par contre, des coordonnées d'un établissement (par exemple, « Établissement XXX » avec son adresse postale, le numéro de téléphone de son standard et un courriel de contact générique « legtaXXX@educagri.fr ») ne sont pas des données personnelles.

Un document peut contenir des renseignements personnels même en utilisant des pseudos, voire aucun nom.

Par exemple un enseignant qui affiche des notes ou des résultats de tests d'une manière qui permet de relier ces résultats aux élèves, divulgue aussi des renseignements personnels.

Tout traitement de données à caractère personnel, mis en œuvre dans un établissement scolaire, doit **faire l'objet d'une inscription sur le registre des activités de traitement** tenu par le responsable de traitement (chef d'établissement ou directeur de structure) désigné au sein de l'établissement.

CONSEILS UTILES
POUR RESPECTER LE RGPD DANS LE CADRE DE VOS ACTIVITÉS

1- NE COLLECTEZ QUE LES DONNÉES VRAIMENT NÉCESSAIRES POUR ATTEINDRE VOTRE OBJECTIF

Les données sont collectées dans un but bien déterminé et légitime, et ne sont pas traitées ultérieurement de façon incompatible avec cet objectif initial.

— Exemple 1 - Le fichier de gestion administrative et pédagogique des élèves ne peut pas être utilisé à des fins commerciales ou politiques.

Le principe de finalité limite la manière dont vous pourrez utiliser ou réutiliser ces données dans le futur, et évite la collecte de données « au cas où ».

Le principe de minimisation limite la collecte aux seules données strictement nécessaires à la réalisation de votre objectif.

— Exemple 2 - Demander le revenu des parents de l'élève pour recevoir la « newsletter » de l'établissement n'est ni pertinent ni nécessaire au regard de la finalité poursuivie par le traitement.

LES BONNES QUESTIONS À SE POSER

— Quel est le but de mon fichier ? (À quoi va-t-il servir ?)

— Est-ce légitime, notamment au regard de mes missions et des droits et libertés des personnes ?

— Comment présenter cette finalité pour la rendre compréhensible par tous ?

2- SOYEZ TRANSPARENT

Les personnes doivent être clairement informées de l'utilisation qui sera faite de leurs données dès leur collecte. Les données ne peuvent en aucun cas être collectées à leur insu.

Les personnes doivent également être informées :

— de l'identité et des coordonnées du responsable de traitement, (chef d'établissement),

— des coordonnées du délégué à la protection des données (DRTIC en DRAAF pour les établissements d'enseignement public),

— des finalités du traitement,

— de la base juridique du traitement,

— du caractère obligatoire ou facultatif du recueil des données,

— des conséquences pour la personne en cas de non-fourniture des données,

— du droit de retirer son consentement à tout moment,

— des destinataires des données,

— de la durée de conservation des données,

— du droit des personnes concernées (opposition, accès, rectification, effacement, limitation),

— du droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL).

3- ORGANISEZ ET FACILITEZ L'EXERCICE DES DROITS DES PERSONNES

Vous devez organiser des modalités permettant aux personnes d'exercer leurs droits et répondre dans les meilleurs délais à leurs demandes de consultation ou d'accès, de rectification ou de suppression des données, voire d'opposition, sauf si le traitement répond à une obligation légale (par exemple, un administré ne peut s'opposer à figurer dans un fichier d'état civil). Ces droits doivent pouvoir s'exercer par voie électronique à partir d'une adresse dédiée.

Contactez le délégué à la protection des données ou DPO de votre organisation, à savoir le DRTIC pour l'enseignement agricole public, ou votre fédération pour les établissements privés.

4- FIXEZ DES DURÉES DE CONSERVATION

Les données doivent être conservées pour la gestion courante, seulement le temps strictement nécessaire à la réalisation de l'objectif poursuivi, puis être détruites, anonymisées ou archivées dans le respect des obligations légales applicables en matière de conservation des archives publiques.

— Exemple - Les informations collectées dans le cadre de l'organisation d'un examen sont conservées pour la durée de la session de l'examen. Au-delà, les données peuvent être archivées, sur un support distinct. La durée de conservation déclarée dans le dossier de formalité adressé à la CNIL ou dans le registre du Correspondant Informatique et Liberté (CIL) doit correspondre à la période durant laquelle les données restent accessibles ou consultables directement par le personnel, par opposition avec la période d'archivage des données, pendant laquelle celles-ci ne sont plus destinées à être utilisées à des fins de gestion et sont, de ce fait, conservées sur un support distinct au sein d'un service d'archives.

LES BONNES QUESTIONS À SE POSER

— Jusqu'à quel moment ai-je vraiment besoin des données pour atteindre l'objectif fixé ?

— Ai-je des obligations légales de conserver les données pendant un certain temps ?

— Dois-je conserver certaines données en vue de me protéger contre un éventuel contentieux ? Lesquelles ?

— Jusqu'à quel moment puis-je faire valoir ce recours en justice ?

— Quelles informations doivent être archivées ? Pendant combien de temps ?

— Quelles sont les règles de suppression des données ?

— Quelles sont les règles d'archivage des données ?

...

2.2 LA PROTECTION DE LA VIE PRIVÉE ET DU DROIT À L'IMAGE

La protection de la vie privée relève d'un droit fondamental qui vise à garder secrète l'intimité de son existence, afin d'éviter toute atteinte à son intégrité physique ou morale. Si l'on se réfère à l'article 9 du code civil « chacun a droit au respect de sa vie privée », ce qui implique que **chacun a le droit de s'opposer à l'utilisation de son image**. Or, de nombreux matériaux pédagogiques sont construits à partir d'images de personnes ou de biens, ce qui nous amène à distinguer les différents « cas d'image » et la règle à laquelle ces cas se rapportent.

CAS CONCERNANT L'IMAGE D'UNE PERSONNE

Par principe, **aucune publication de l'image d'une personne ne peut être réalisée sans son autorisation** si la personne est reconnaissable ou identifiable, même si l'image a été prise dans un lieu public comme un jardin, une université, dans la rue… Cette règle est également valable pour tout élément qui la caractérise comme sa voix, son nom, son pseudo, et ce, quel que soit le support concerné : blog, réseau social, affiche, site Internet d'un établissement…

Il est donc nécessaire de recueillir le consentement écrit de l'apprenant ou de son représentant légal s'il est mineur, pour la capture d'images au cours d'un voyage scolaire ou avant d'enregistrer un cours en présentiel ou en visioconférence.

Cette autorisation, écrite et signée, doit préciser les éléments caractéristiques de la diffusion afin de s'assurer que la personne a donné son consentement à toutes les utilisations qui seront faites de l'image. Par exemple, le seul fait d'avoir accepté d'être pris en photo ne vaut pas acceptation que l'image soit utilisée à des fins autres que celles prévues dans l'autorisation.

Pour illustration, l'autorisation doit contenir :

- les nom et prénom de la personne photographiée ou filmée et ceux de la personne à qui est donnée l'autorisation (par exemple, l'établissement scolaire),
- la destination des images ou vidéos (adresse de site Internet, ou applications, etc.),
- le cadre d'utilisation et sa finalité (article d'information, présentation de l'établissement, journal en ligne, réseaux sociaux, etc.) ; le caractère gratuit ou non de l'autorisation,
- le territoire sur lequel cette autorisation de diffusion est accordée ; pour Internet, il s'agit de préciser le ou les sites,
- la durée de l'autorisation.

La preuve de l'autorisation, en cas de litige, incombe à celui qui publie l'image.

Il est à noter que le consentement des personnes n'est pas requis pour des prises de vues liées un événement d'actualité, ou pour une personnalité publique dans l'exercice de ses fonctions (ministres, députés, artistes) qui relèvent dans ce cas précis du droit à l'information. Toutefois, la diffusion d'images doit toujours respecter la dignité des personnes, elles ne doivent pas montrer des situations dégradantes ou humiliantes.

CAS CONCERNANT L'IMAGE D'UN BIEN MOBILIER OU IMMOBILIER

Le propriétaire d'un bien (maison, jardin, voiture...) ne bénéficie pas d'un droit exclusif sur l'image de celui-ci, son autorisation pour une diffusion de son image n'est en principe pas requise[1]. Toutefois, le propriétaire peut reprocher à l'utilisateur d'une photographie de son bien, une exploitation qui lui causerait un trouble anormal ou qui porterait atteinte à sa vie privée. Par contre, si le bien n'est pas visible depuis l'espace public, l'accord du propriétaire pour une exploitation de l'image de son bien est nécessaire.

Si le bien est une œuvre, le droit à l'image se heurte au droit d'auteur en faveur de l'architecte ou de l'artiste l'ayant conçu.

Si l'œuvre (fontaine, sculpture, tableau) constitue le sujet principal de l'image, alors le consentement des auteurs est requis. Toutefois, le législateur *via* la loi pour une République Numérique du 07/10/2016, dans son article 38, vient modifier cette règle et consacre la liberté de panorama. Cette loi autorise les reproductions et représentations d'œuvres architecturales et de sculptures, placées en permanence sur la voie publique, réalisées par des personnes physiques, à l'exclusion de tout usage à caractère commercial.

1- Attention, ce principe n'est pas absolu, un propriétaire peut saisir la justice et obtenir gain de cause s'il démontre que la publication d'une image de son bien lui a causé préjudice.

CONSEILS UTILES

POUR RESPECTER LE DROIT À L'IMAGE DANS LE CADRE DE VOS ACTIVITÉS

- Avertir les participants à un événement que des photos / vidéos / enregistrements audio sont susceptibles d'être pris, et à quelles fins ils sont destinés.
- Éviter les prises de vues qui ne mettent pas les apprenants ou vos collègues à leur avantage.
- Préciser, lors de la diffusion, que les images ont fait l'objet d'une demande d'autorisation.
- Comprendre que tout ce qui n'est pas prévu par l'autorisation n'est pas autorisé.
- Ne pas associer la photographie d'une personne à tout élément permettant son identification.
- Être vigilant aux techniques de brouillages type floutage ou autres qui peuvent ne pas être suffisantes pour masquer une identité (tatouages, voix, environnement).
- S'interroger sur la règle en vigueur pour un bien susceptible d'être protégé par le droit d'auteur.
- Conserver les autorisations le temps nécessaire, c'est-à-dire tant que la diffusion des images est susceptible de circuler.

BIBLIOTHÈQUE D'IMAGES : MÉDIATHÈQUE DU MINISTÈRE CHARGÉ DE L'AGRICULTURE

- 400 films à regarder en ligne (films réalisés de 1947 à 1962)
- De nombreuses photographies anciennes (à partir de 1950)
- 30 000 photos contemporaines
- Des animations, flyers, affiches, brochures, infographies…

COMMENT Y ACCÉDER ?

Pour les agents du ministère chargé de l'agriculture, dotés d'une adresse en agriculture.gouv.fr, ces contenus sont en téléchargement libre.

Un accès rapide est proposé en page d'accueil de l'Intranet.

Pour les autres agents et pour le grand public, l'accès se fait *via* : store.agriculture.gouv.fr/

ou *via* le contact de la Dicom du ministère.

Le téléchargement est possible après création d'un compte permettant de réaliser des commandes.

2.3 LES RÈGLES DE LA PROPRIÉTÉ LITTÉRAIRE ET ARTISTIQUE

Comme vu précédemment, les séquences pédagogiques peuvent faire appel à des contenus littéraires et artistiques (image, photo, vidéo, texte, musique) susceptibles d'être protégés par le droit d'auteur. Toutefois, leur utilisation peut entrer dans le champ des exceptions prévues par la loi.

DÉFINITION ET CARACTÉRISTIQUES DU DROIT D'AUTEUR

Le droit d'auteur impose à tout utilisateur d'une œuvre d'obtenir l'autorisation de l'auteur ou de celui qui détient les droits, pour l'utiliser, (cf. en annexe la liste des organismes de gestion collective des droits d'auteur). Or la notion d'œuvre est extrêmement large[1] et le droit s'applique dès la création, sans nécessité de procéder à un dépôt.

Cela signifie que lorsqu'on utilise un matériau produit par autrui, il faut tenir compte du droit d'auteur :

1- La loi cite des exemples d'œuvre mais la liste n'est pas limitative (écrits littéraires, artistiques et scientifiques, allocutions, œuvres dramatiques, œuvres audiovisuelles, œuvres graphiques, compositions musicales, dessins, œuvres d'architecture, œuvres d'art appliqué, logiciels, etc.).

— quel que soit le sujet du contenu (même un contenu technique, scientifique, une monographie, une infographie, une prestation orale, un site Web, une illustration, etc.) ;

— quelle que soit la qualité du contenu ;

— même si l'auteur n'indique pas avoir « déposé » le contenu ;

— même en l'absence de toute mention de type « copyright » ou « tous droits réservés ».

Par prudence, l'utilisateur doit considérer que tout contenu est potentiellement soumis au droit d'auteur et donc que son utilisation nécessite une autorisation.

Le fait que le contenu soit soumis au droit d'auteur ne signifie pas automatiquement que son utilisation ouvre droit à rétribution car celle-ci peut être gratuite, voire donnée par avance à tout le monde (licences libres).

Tout utilisateur qui ne dispose pas d'autorisation d'utilisation d'une œuvre commet ainsi un acte délictuel (contrefaçon), et s'expose, si les auteurs le poursuivent, à une condamnation au paiement de dommages-intérêts et/ou à des sanctions pénales. Pour s'en prémunir, il faut obtenir une autorisation écrite qui évite tout malentendu et qui permet de s'assurer que le titulaire des droits a accepté les utilisations qui seront faites de son œuvre.

Il existe toutefois des cas particuliers, qui nécessitent que l'on s'y attarde pour comprendre quelle règle de droit s'applique.

SI L'ŒUVRE APPARTIENT AU DOMAINE PUBLIC

Au décès d'un auteur, le droit d'auteur persiste au bénéfice de ses ayants droit (ex. : héritier) pendant l'année civile en cours et les soixante-dix années qui suivent. À l'issue de cette période de protection, plus aucune autorisation n'est nécessaire pour utiliser une œuvre, même à titre commercial. C'est ce que l'on appelle l'entrée dans le domaine public.

Si l'œuvre est entrée dans le domaine public, l'utilisateur doit toutefois rester vigilant sur certains points :

— les adaptations, œuvres dérivées[2] ou incorporant cette œuvre peuvent être toujours soumises au droit d'auteur : par exemple l'utilisation d'un film récent tiré d'un roman entré dans le domaine public nécessite l'autorisation du titulaire des droits du film ;

— l'interprétation de l'œuvre que l'on souhaite utiliser peut encore être protégée au titre du droit des artistes-interprètes : par exemple, l'utilisation d'une musique de film ou d'une chanson dans une vidéo ;

— l'œuvre que l'on souhaite utiliser est toujours protégée par le droit moral, perpétuel, inaliénable et imprescriptible, qui permet de veiller à la paternité et au respect de l'intégrité de l'œuvre. Ainsi tout auteur pourra toujours s'opposer aux exploitations portant atteinte à son honneur ou à sa réputation ou aux modifications dénaturant son œuvre, même si l'œuvre a été déposée sous licence Creative Commons la plus ouverte.

2- Œuvre créée à partir d'une ou plusieurs œuvres préexistantes.

LES EXCEPTIONS AUTORISÉES

Il est tout à fait possible d'utiliser des œuvres qui ne sont pas tombées dans le domaine public sans devoir demander l'autorisation de l'auteur (ou du titulaire des droits) ou devoir verser une compensation financière en contrepartie. C'est le cas lorsque l'utilisation que l'on souhaite faire de l'œuvre est couverte par les exceptions et limitations prévues par l'article L.122-5 du code de la propriété intellectuelle. Ces exceptions et limitations peuvent concerner, par exemple :

- les analyses et courtes citations d'œuvres justifiées par le caractère critique, polémique, pédagogique, scientifique ou d'information, de l'œuvre à laquelle elles sont incorporées (mémoire, exposé…) sous réserve que soient indiqués l'auteur et la source ;
- l'utilisation des revues de presse, sous réserve que soient indiquées les sources ;
- la création de formats accessibles pour les personnes ayant des difficultés de lecture des textes imprimés, par des personnes morales ou des établissements ouverts au public, tels les bibliothèques, les archives, les centres de documentation et les espaces culturels multimédias, à des fins non lucratives, dans la mesure du handicap et en vue d'une consultation strictement personnelle ;

- la copie à usage privé : cette exception est d'application limitée. Elle ne vise en pratique que la copie effectuée pour les besoins personnels de celui qui la réalise. Elle ne s'applique pas aux copies d'œuvres d'art destinées à être utilisées pour des fins identiques à celles pour lesquelles l'œuvre originale a été créée, ni aux logiciels où seule la copie de sauvegarde est permise, ni aux bases de données numériques ;
- les représentations privées et gratuites dans le cercle familial.

Il existe également des utilisations autorisées sous certaines conditions à des fins exclusives d'illustration dans le cadre de l'enseignement et de la recherche à destination d'un public majoritairement composé d'élèves, d'étudiants, d'enseignants ou de chercheurs, sans aucune exploitation commerciale et compensée par une rémunération négociée (exception pédagogique), à des fins de conservation, ou destinées à préserver les conditions de sa consultation à des fins de recherche ou d'études privées par des particuliers sur des terminaux dédiés par des bibliothèques, des musées ou services d'archives.

Ces exceptions pourront faire l'objet de compléments ultérieurs de ce guide, car les nombreuses limitations nécessitent d'être détaillées plus avant.

3

ENGAGEMENTS DE L'ÉTABLISSEMENT

L'établissement doit s'efforcer dans la mesure du possible de maintenir accessibles les services numériques qu'il propose de manière permanente, mais n'est tenu à aucune obligation d'y parvenir. Il peut donc interrompre l'accès des services, notamment pour des raisons de maintenance et de sécurité informatique ou pour toute autre raison, sans être tenu pour responsable des conséquences de ces interruptions aussi bien pour l'utilisateur que pour les tiers. Il est par contre du devoir de l'établissement de tenir les utilisateurs informés de la durée et de la nature de ces interruptions.

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 numériques.

3.1 RÈGLES D'USAGE CONCERNANT L'UTILISATION DE LA MESSAGERIE INSTITUTIONNELLE

ADRESSAGE

Tout message émanant d'une adresse institutionnelle peut engager l'établissement. L'utilisateur doit donc s'assurer qu'il est autorisé à l'adresser au vu de ses fonctions. Si tel n'est pas le cas, il transfère le message à sa hiérarchie.

L'utilisateur utilise la règle des copies pour informer sa hiérarchie. En retour, les messages en copie (CC) permettent à la hiérarchie d'informer l'ensemble des agents concernés. La pratique des **copies cachées** (CCI) est à proscrire, car elle ne permet pas une circulation transparente de l'information.

PIÈCES JOINTES

L'utilisateur porte une attention particulière à la taille et au contenu des fichiers transmis. En règle générale, si la taille excède la limite prescrite par l'administrateur, le message est bloqué et éliminé du réseau. Toutefois, au ministère chargé de l'agriculture, les utilisateurs de la messagerie institutionnelle (Mél) peuvent envoyer un message volumineux (< 5 Mo). Si les pièces jointes du message sont trop volumineuses, un lien de téléchargement de ces pièces sera automatiquement envoyé grâce à l'outil « Mélanissimo ». Il est possible de choisir la durée pendant laquelle le lien permettant d'accéder aux pièces jointes sera actif (entre 3 et 30 jours).

N. B. - L'utilisation de la messagerie ne doit pas se faire au détriment des sites collaboratifs de partage de documents (type RESANA) qui conduisent à soulager la messagerie ainsi qu'à développer le partage et le fonctionnement en réseau.

CARACTÈRE DU CORPS DU MAIL

Si le contenu a un caractère confidentiel, l'utilisateur doit demander à l'administrateur de lui fournir une solution de cryptage. Il convient de s'assurer que le destinataire dispose du même logiciel de cryptage pour pouvoir lire le

message ou lui indiquer le logiciel de cryptage utilisé. Le ministère chargé de l'agriculture utilise le logiciel gratuit ZEDFREE.

Par défaut, les courriels ou les fichiers enregistrés sur un poste de travail ont un caractère professionnel. L'établissement peut les lire, tout comme il peut prendre connaissance des sites consultés, y compris en dehors de la présence de l'utilisateur.

Si le message a un caractère privé, l'utilisateur doit y faire figurer la mention « privé » ou « personnel », et demander à son correspondant externe d'agir de même.

La distinction est importante puisque seuls les fichiers ou courriels professionnels peuvent être ouverts par l'établissement, même en l'absence du salarié concerné. En effet, l'employeur est en droit de contrôler et limiter l'utilisation d'Internet (dispositifs de filtrage, détection de virus…) et de la messagerie (outils de mesure de la fréquence des envois et/ou de la taille des messages, filtres « anti-spam »…) afin de :

- sécuriser les réseaux qui pourraient subir des attaques (virus, malware, rançongiciel…) ;
- limiter les risques d'abus d'une utilisation trop personnelle d'Internet ou de la messagerie (consultation de sa messagerie personnelle, achats de produits, visionnage de vidéos, discussions sur les réseaux sociaux…) ;

Quels que soient le destinataire, l'objet du mail ou la nature des échanges, aucun message professionnel ou privé ne doit comprendre des éléments de nature offensante, diffamatoire, injurieuse ou à connotation pornographique, sexiste ou raciste.

À RETENIR

Les courriels ou les fichiers enregistrés sur un poste de travail ont **un caractère professionnel**.

L'établissement peut les lire, tout comme il peut prendre connaissance des sites consultés, **y compris en dehors de la présence de l'utilisateur**.

Les fichiers ou courriels doivent contenir expressément la mention **« PERSONNEL »** ou les mentions **« PRIVÉ »** ou **« PERSO »** pour revêtir ce caractère. Ils ne peuvent pas être lus par l'établissement **sans l'accord de l'utilisateur**.

L'intitulé du fichier **« Mes documents »** est insuffisant à lui donner un caractère personnel. Le fait que les fichiers soient verrouillés par un code d'accès est insuffisant pour leur donner un caractère personnel.

La Cour de cassation considère d'ailleurs, en pareille situation, que si des fichiers stockés sur l'ordinateur de bureau ont été verrouillés par l'utilisateur avec un code d'accès, il lui appartiendra de le communiquer à l'établissement pour qu'il puisse y accéder.

Source : https://www.cnil.fr/en/node/15840

3.2 RÈGLES D'USAGE EN MATIÈRE DE COMMUNICATION NUMÉRIQUE DE L'ÉTABLISSEMENT

La publication d'informations sur le site Internet de l'établissement engage la responsabilité éditoriale des différents acteurs qui doivent assumer les conséquences de la diffusion d'informations aussi bien d'un point de vue civil que pénal. En effet, même si la portée d'un écrit paraît neutre pour son auteur, les contenus publiés peuvent porter atteinte à l'honneur ou à la réputation d'apprenants ou d'enseignants, atteinte à la vie privée (photos, informations intimes, image…), ainsi qu'aux droits d'auteur…

Pour se prémunir de mésusages, quelques règles simples doivent être connues.

MENTIONS LÉGALES (ÉGALEMENT VALABLES POUR UN BLOG)

Le directeur de la publication, au titre des services de communication au public proposé par l'établissement, est son représentant légal. Il s'agit donc du chef de l'établissement.

Le site Internet d'un établissement scolaire est un site Internet professionnel non commercial, et doit donc à ce titre comporter les mentions légales suivantes, conformément aux dispositions de la loi du 21 juin 2004 pour la confiance dans l'économie numérique :

- Nom, prénom, adresse géographique, adresse de courrier électronique, numéro de téléphone du responsable de publication ;
- Nom, dénomination ou raison sociale, adresse et le numéro de téléphone de l'hébergeur du site.

Si l'établissement collecte des données à caractère personnel *via* un formulaire par exemple, il est obligé d'informer les personnes sur leurs droits (https://www.cnil.fr/fr/comprendre-vos-droits).

Si le site Web dépose et lit des cookies, l'éditeur doit obligatoirement informer les internautes de la finalité des cookies, obtenir leur consentement, fournir aux internautes un moyen de les refuser.

Concernant la protection intellectuelle des contenus du site Internet, il est également obligatoire de rappeler les mentions relatives au droit d'auteur :

- « Aucune reproduction sans autorisation explicite de l'auteur n'est possible » ;
- ou une mention du type « Tous les contenus du site Web sont mis à disposition sous licence Creative Commons » ;
- ou rappeler le nom de l'auteur/autrice et/ou sa source sous chaque œuvre protégée (photo notamment), ou de prévoir une page répertoriant tous les crédits, et de s'assurer qu'on détient les droits d'utiliser les œuvres.

L'établissement s'engage à détenir et conserver les données permettant l'identification de toute personne ayant contribué à la communication au public d'un contenu dans le cadre des services proposés, conformément aux dispositions de l'article 6-II de la loi du 21 juin 2004 pour la confiance dans l'économie numérique. Ces informations conservées pendant **le temps limité de cette communication** sont strictement destinées aux éventuels besoins des autorités judiciaires.

À RETENIR

Le chef d'établissement est responsable de toute publication mise en ligne sur le site de l'établissement.

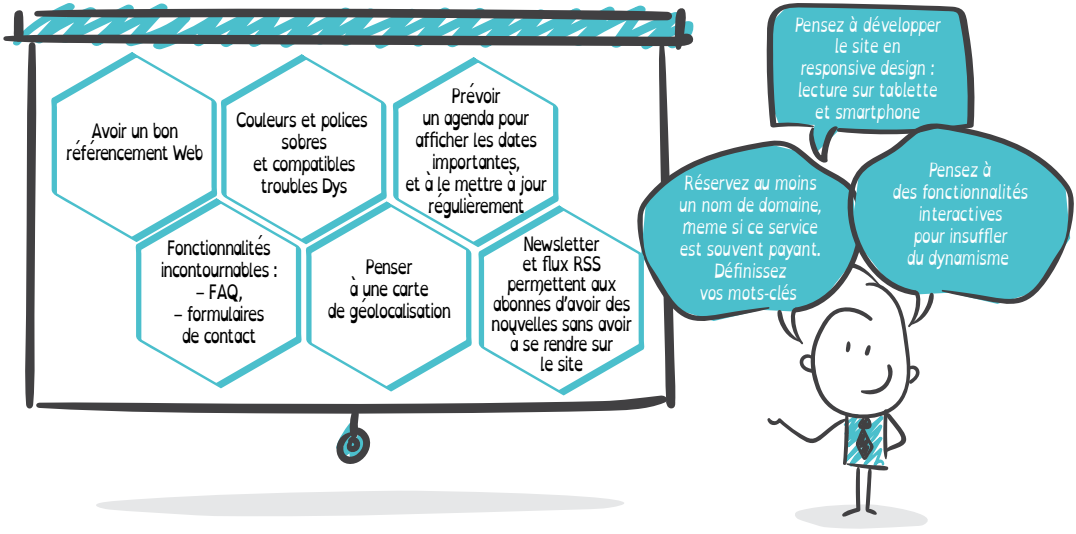
Il doit veiller à ce que les publications en ligne n'incluent aucun contenu illégal.

L'établissement doit être en mesure de fournir les informations permettant l'identification de toutes les personnes ayant contribué à la publication mise en ligne.

RÈGLES DE FORME

Un site Web est une formidable vitrine pour les établissements puisqu'il permet à la fois d'informer le public sur les caractéristiques de l'établissement mais également de valoriser ses actions éducatives ou pédagogiques, lui assurant ainsi une image dynamique et positive, parfois concurrencé par des pages Facebook ou autres.

Le site Web de l'établissement doit cependant rester le moyen de communication institutionnel avec, pour l'usager, la garantie d'entrer dans un univers qui est orienté par les finalités associées à l'activité d'enseignement. *« Le site Web de l'établissement devrait donc désormais être repensé en lien avec les autres activités numériques au sein de l'établissement. La partie information de ce site est donc un écho de l'intérieur (contrôlé et sécurisé) vers l'extérieur (ouvert à tous). C'est aussi un écho de l'extérieur vers l'intérieur par le biais de l'attirance de ce qu'il montre à voir et des méthodes qu'il utilise pour attirer les lecteurs, les visiteurs. »* Bruno Devauchelle, 2012, Site du Café pédagogique, http://www.cafepedagogique.net/lexpresso/



Ainsi, le site d'un établissement doit répondre à des exigences bien particulières en matière d'ergonomie. Sur les contenus portés à la connaissance du public, les informations doivent être vérifiées et validées par le responsable éditorial afin de s'assurer d'une unité éditoriale et de la conformité des informations.

Enfin, s'il y a **des enjeux de recrutement**, le site d'un établissement **doit avoir un bon référencement** pour apparaître en premier lors de recherches avec quelques mots-clés (ex. : lycée agricole, ville ou lycée agricole, région).

3.3 PROTECTION DES JEUNES UTILISATEURS

La majorité numérique est fixée en France à 15 ans[1], elle correspond à l'âge auquel la loi française considère un jeune comme le propriétaire de ses données personnelles. Il est alors en mesure d'accepter ou non que des services tiers aient accès à ses données pour les collecter à des fins commerciales. Avant la majorité numérique, le jeune doit obtenir l'accord préalable de son représentant légal pour s'inscrire sur les réseaux sociaux ou avoir accès à une boîte mail par exemple.

L'établissement et les équipes pédagogiques ont le devoir de protéger leurs apprenants en les formant et en les conseillant dans leur utilisation d'Internet et des outils numériques.

Il incombe ainsi à l'établissement et aux équipes pédagogiques de garder la maîtrise des activités proposées par l'établissement, en mettant tout en œuvre pour éviter toute fuite de données personnelles, toute publication d'articles interprétatifs ou pouvant porter atteinte à l'image, l'intégrité d'un ou plusieurs apprenants.

Il appartient également à l'établissement et aux équipes pédagogiques de veiller à une organisation d'activités offrant de bonnes conditions de sécurité numérique. Dans ce cadre, des logiciels permettant d'autoriser ou non l'accès à certains sites seront mis en œuvre. Toute ouverture de sites ou de services numériques est soumise à l'approbation de la direction de l'établissement.

LE RECOURS AUX PROXYS

Les serveurs proxys[2] sont notamment utilisés pour assurer les fonctions suivantes :

- l'accélération de la navigation : mémoire cache, compression de données, filtrage des publicités ou des contenus lourds (Java, Flash),
- l'historique des requêtes,
- la sécurité du réseau local,
- le filtrage et l'anonymat.

1- Article 45 de la loi Informatique et Libertés (âge minimal de consentement pour les enfants en France)

2- Un proxy (ou serveur mandataire en français) est un filtre qui permet de sécuriser l'accès à Internet, en évitant les contenus choquants ou inadaptés.

L'établissement s'engage à informer l'utilisateur, d'une manière précise, sur les mécanismes de protection mis en œuvre dans le cadre de la fourniture des services Internet / Intranet. Cette information est souvent réalisée dans la charte informatique que l'établissement a contractualisée avec l'enseignant.

EXEMPLES DE TRAÇAGE D'INFORMATIONS SUR UNE JOURNÉE TYPE, SELON LA CNIL

Au lever, vous demandez à votre assistant vocal de vous lire vos derniers courriers électroniques pendant que vous vous habillez pour vous rendre au travail.

Dans les transports en commun, vous vous rendez sur une plateforme de microblogging avant de consulter un site d'information en ligne renommé.

Sur le chemin, vous vous arrêtez prendre une tasse de café et en profitez pour publier une photo de votre petit-déjeuner en « taguant » l'établissement dans lequel vous vous trouvez sur votre réseau social préféré.

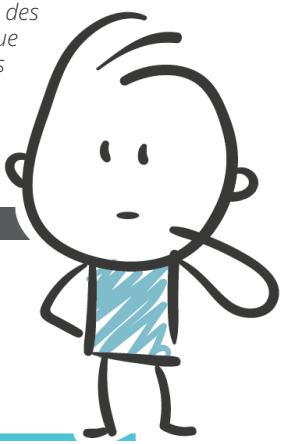
Durant la pause déjeuner, vous vous rendez sur un site d'e-commerce afin de rechercher une nouvelle paire de lunettes de ski pour votre week-end à la montagne avant de vous rendre sur votre réseau social pour partager vos plans avec vos amis.

Il ne s'agit que d'une poignée de services, mais les données relatives à ces activités et associées à votre profil ont potentiellement été collectées non pas par une dizaine d'acteurs avec lesquels vous avez eu une interaction en ligne, mais par plus d'une centaine d'entreprises différentes en l'espace d'une journée.

Si les sites Web et les applications avec lesquels vous interagissez sont visibles, d'autres sociétés peuvent suivre vos activités et collecter des données relatives à votre navigation en ligne sans que cela ne soit nécessairement évident pour vous, pour vous afficher de la publicité.

Plus tard dans la journée, vous commencez à voir des messages sponsorisés sur votre plateforme de microblogging à propos de week-ends à la montagne, des annonces publicitaires sur votre réseau social pour les lunettes de ski que vous avez cherchées, et des suggestions de nouveaux cafés à découvrir près de votre lieu de travail.

Toutes ces traces de navigation ont été laissées sur Internet *via* les cookies.



Source : https://www.cnil.fr/en/node/119436

BIEN COMPRENDRE LES COOKIES POUR SAVOIR LES GÉRER

Un « cookie » est un petit fichier texte transmis par un site Web sur lequel vous naviguez, déposé sur votre terminal (ordinateur, tablette, smartphone…). Votre navigateur Web le conservera alors pendant une certaine durée, et renverra au serveur Web les informations enregistrées chaque fois que vous vous reconnecterez au site en question.

Les cookies ont de multiples utilités : ils mémorisent vos choix de personnalisation, des informations pour vous éviter de les ressaisir, un identifiant pour suivre votre navigation à des fins statistiques et d'amélioration d'un service, le contenu de votre panier d'achat dans le cas d'un site marchand…

À partir des habitudes de navigation, les entreprises peuvent prédire le sexe, le revenu, la composition familiale, les habitudes d'achat, les centres d'intérêt et les opinions politiques des individus. Un simple test avec l'outil « Cookieviz » développé par la CNIL permet de constater l'ampleur de cette collecte de données.

Afin de laisser le moins de traces possibles, il peut paraître utile d'utiliser un VPN, même si cet outil peut parfois ralentir la connexion Internet et la rendre instable. Il est également utile d'exercer son droit au respect de la vie privée en refusant certaines catégories spécifiques de cookies (préférences, statistiques et marketing).

3.4 PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL DE L'UTILISATEUR

En application des dispositions de la loi informatique et libertés n° 78-17 du 6 janvier 1978 et de la directive européenne 95/46/CE relative à la protection des données personnelles et à la libre circulation de ces données du 24 octobre 1995, l'établissement s'engage à respecter le Règlement Général sur la Protection des Données (RGPD). Il garantit notamment à l'utilisateur :

- de n'utiliser les données à caractère personnel le concernant que pour les strictes finalités pour lesquelles elles sont collectées (ouverture du compte d'accès, contrôles techniques définis à l'article 3-7…) ;
- de lui communiquer les finalités et la destination des informations enregistrées et leur durée de conservation, laquelle ne peut en tout état de cause excéder ce qui est nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou traitées ;
- de lui garantir un droit d'accès et de rectification aux données le concernant.

AU TRAVERS DU RGPD, QUELLE EST L'INTENTION DU LÉGISLATEUR ?

Ces règles ont pour visée de protéger notre vie privée en choisissant avec qui nous souhaitons partager les informations nous concernant. Lors de nos activités quotidiennes (travail, navigation sur Internet, achats…) les données transmises sont attentivement suivies par des sociétés privées dont l'objectif est de profiler les individus, afin de leur proposer des services adaptés à leurs besoins réels ou supposés.

L'autre champ d'intervention n'est pas économique mais lié à la prévention de toutes formes de recherche d'influence tant privée qu'étatique sur un groupe d'individus.

Dans l'enseignement agricole comme dans tout autre organisme public ou privé, un délégué à la protection des données (DPO[1]) doit veiller au respect du RGPD par les responsables des traitements de données personnelles (les directeurs d'établissements), et par les sous-traitants et prestataires prenant part à ces traitements.

RÔLE DU DÉLÉGUÉ À LA PROTECTION DES DONNÉES PERSONNELLES

Ce rôle, défini aux articles 37 à 39 du RGPD, est exercé dans l'enseignement agricole public par les DRTIC (Délégués régionaux aux technologies de l'information et de la communication) et couvre 3 missions principales :

- apporter information et conseil auprès des responsables de traitement et des porteurs de la démarche au sein de l'EPLEFPA,
- s'assurer de la conformité de la démarche engagée par l'établissement,
- assister le responsable de traitement en cas de contrôle, coopérer avec la CNIL et être le point de contact de celle-ci.

Chaque établissement public a l'obligation de déclarer son DPO auprès de la CNIL.

Il est à noter que le DPO a essentiellement un rôle de conseil, il n'y a aucun transfert de responsabilité du chef d'établissement vers le DPO.

ACTIONS POUR L'ÉTABLISSEMENT

Chaque EPLEFPA nomme son DPO conformément à l'article 37 du RGPD et à l'arrêté du DRAAF. Il identifie ensuite le porteur de la démarche et lui rédige une lettre de mission. Ce dernier conduit la mise en conformité RGPD sous la responsabilité de son responsable de traitement.

Le DPO forme et conseille les Responsables de Traitements et leur(s) représentant(s), il anime ce groupe, apporte et partage son expertise à chaque étape avec des objectifs :

- de montée en compétences de ces porteurs de la démarche,
- d'identification des actions à réaliser sur chacun des sites,
- de recherche de mutualisation,
- de conseil à la mise en œuvre…

La première action doit mettre en place une organisation interne pour conduire la mise en conformité de l'établissement public.

La seconde consiste à nommer le représentant du Directeur d'EPL et le DPO auprès de la CNIL.

1- DPO est l'acronyme anglais pour **data police officer**. Le rôle de délégué à la protection des données personnelles est confié à d'autres personnes pour les composantes CNEAP, UNREP, MFR de l'enseignement agricole.

Il est alors temps de procéder à l'inventaire des traitements de données à caractère personnel mis en œuvre dans l'EPL, puis de prioriser les actions à mener en fonction des risques induits par ces différents traitements.

L'étape suivante consiste à rédiger une fiche de traitement pour chacun d'entre eux puis à l'insérer dans le registre de traitement de l'EPLEFPA, conformément à l'article 30 du RGPD. Lors de cet exercice, il est indispensable de vérifier que les personnes concernées par ces traitements sont correctement informées de leurs droits, par exemple *via* les informations légales sur les formulaires de collecte (Inscriptions, prospections salons…) ainsi que sur les sites Internet.

Lorsque des données personnelles à caractère sensible sont identifiées, une étude d'impact doit être réalisée. Des actions de sensibilisation au RGPD doivent être menées au sein de l'établissement à destination de tous ses personnels.

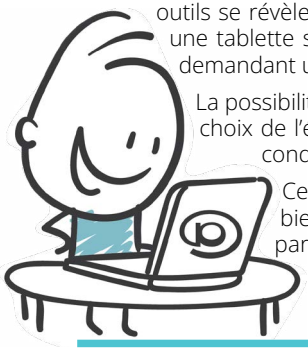
Lors de ces premières étapes, le Directeur, ou son représentant, prend l'attache du DPO académique afin d'être guidé et conseillé. Il est important, pour chaque étape, de documenter les travaux afin de pouvoir établir la preuve de la mise en conformité.

Afin d'assurer la sécurité de leur réseau et/ou de leurs ressources informatiques, les établissements peuvent être conduits à mettre en place des instruments pour sécuriser l'utilisation des outils informatiques mis à disposition des utilisateurs, comme des proxys ou VPN par exemple.

3.5 CAS PARTICULIER DU BYOD EN CLASSE

Le « BYOD » est l'acronyme de l'expression anglaise *« Bring Your Own Device »*, autrement dit « Apportez votre propre équipement » sous-entendant d'apporter du matériel numérique personnel dans un contexte professionnel ou à l'école comme, par exemple, son ordinateur, son smartphone, sa caméra portative, son disque dur externe…

Le BYOD propose ainsi une alternative intéressante à l'utilisation d'outils disponibles dans l'établissement. En fonction de l'activité à réaliser, certains outils se révèlent plus pertinents que d'autres, comme, par exemple, une tablette sera plus adaptée pour une activité extérieure mobile demandant une géolocalisation précise.



La possibilité d'utiliser des outils personnels relève avant tout d'un choix de l'établissement qui peut tout aussi bien l'autoriser sous conditions, ou l'interdire.

Cette décision devra cependant être prise de manière à bien évaluer les intérêts et les inconvénients présentés par cet usage qui brouille la frontière entre vie personnelle et vie professionnelle ou de classe. De plus, il est

indispensable de se prémunir contre la compromission générale du système d'information de l'établissement (intrusion, virus, chevaux de Troie, etc.), ce qui n'est pas de la compétence première d'un enseignant. Les professeurs TIM sont, à ce moment, la ressource la plus à même de répondre aux questions techniques des enseignants sur ces sujets.

Recourir au BYOD ne dédouane pas des obligations auxquelles les traitements métiers sont soumis (inscription au registre des traitements et, le cas échéant, analyse d'impact relative à la protection des données). La direction d'établissement devra ainsi autoriser le BYOD dans son établissement si elle a au préalable :

- identifié les risques, en tenant compte des spécificités du contexte (quels équipements, quelles applications, quelles données ?), et elle les a estimés en termes de gravité ;
- déterminé les mesures à mettre en œuvre et les a formalisées dans une politique de sécurité.

La question n'est pas tant de savoir si l'utilisation du BYOD est pertinente ou non, mais de réfléchir à un usage responsable et donc d'agir *a minima* sur des leviers pertinents.

SYNTHÈSE OPÉRÉE À PARTIR DES CONSEILS ISSUS D'UN MOOC

1- L'IMPLICATION DES DIFFÉRENTS ACTEURS

Pour une plus grande chance de succès, le BYOD doit impliquer administration, enseignants, parents et apprenants.

Un projet BYOD **se construit avec la direction de l'établissement et éventuellement le conseil d'administration ou le CEF**[1]. L'accueil en classe d'outils personnels sera facilité si les informations concernant une activité précèdent l'usage, et que des engagements ont été formalisés auprès des différents acteurs (finalités, soins au matériel...).

Le règlement intérieur ou la charte informatique de l'établissement doivent prévoir l'utilisation du BYOD en classe.

2- LA NON-DISCRIMINATION AU MATÉRIEL

Tous les apprenants ne sont pas équipés de matériel, ou de matériel aux performances équivalentes.

Privilégiez les activités qui ne requièrent pas un outil par personne, mais **des usages de type collaboratif** impliquant (binôme/ groupe) avec une articulation classe/ maison ou hors la classe.

3- LA PRISE EN COMPTE DE LA TECHNIQUE : COMPATIBILITÉ ET CONNECTIVITÉ

La diversité des matériels entre apprenants pose la question de la compatibilité des productions lors d'échanges ou de partage entre supports.

L'enseignant devra avoir anticipé cette contrainte, car elle conditionne le choix des activités.

Un ensemble de questions, à la fois administratives et techniques, sera à considérer s'il est souhaité que les apprenants puissent accéder à Internet à partir de leurs données mobiles ou du wifi de l'établissement.

4- LA RESPONSABILISATION DES APPRENANTS

La responsabilisation des apprenants est l'élément essentiel d'une intégration technologique réussie.

L'enseignant doit favoriser des situations d'apprentissage qui permettent le développement de compétences disciplinaires et transversales, mais aussi de construire leur culture numérique. Enseignants et apprenants devront définir ensemble la production souhaitée et les outils envisagés en fonction des contraintes identifiées (technique, usages, sécurité de l'outil...).

1- Conseil de l'éducation et de la formation

4

LE RÔLE D'« ADMINISTRATEUR » EXERCÉ AU SEIN DE L'ÉTABLISSEMENT

Le responsable des systèmes d'information, dénommé « administrateur », assure la direction de toutes les activités liées à la production, au transport et au stockage des données informatiques. Il a accès à toutes les données qui s'échangent tant sur le réseau interne qu'avec l'extérieur.

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 peut être analysée et contrôlée 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'administrateur est ainsi tenu à un strict respect du secret professionnel. La surveillance de l'administrateur ne s'exerce pas sur les dossiers informatiques « privés » ou « personnels », sauf dans le cas d'un dysfonctionnement important.

L'administrateur veille à ce que les matériels et logiciels mis à la disposition des utilisateurs soient conformes aux besoins définis par leur hiérarchie. Concernant leur usage, il peut comptabiliser les temps de connexions, les sites visités, les volumes téléchargés ainsi que toute activité relative à l'usage des matériels informatiques (ordinateurs, tablettes, smartphones, etc.) et serveurs, de la messagerie électronique, d'Intranet et d'Internet. Il réalise des rapports périodiques non personnalisés, transmissibles par voie hiérarchique.

En cas de détection de comportements non conformes à la charte informatique, l'administrateur peut, après en avoir informé personnellement et par écrit l'utilisateur, réaliser une surveillance personnelle dont les résultats sont communiqués à la direction de l'établissement. Dans tous les cas, l'administrateur se garde le droit d'effacer, de comprimer ou d'isoler tout fichier ou toute donnée manifestement en contradiction avec la charte informatique ou qui mettrait en péril la sécurité des moyens informatiques.

L'établissement se réserve, dans ce cadre, le droit de recueillir et de conserver les informations nécessaires à la bonne marche du système, conformément à la durée de conservation des données indiquée dans le dossier de déclaration CNIL ou dans le registre du CIL.

Dans le cadre de ses missions, l'administrateur est autorisé à utiliser un logiciel de prise de main à distance à des fins d'assistance informatique. Afin de garantir la transparence dans l'utilisation de ce type de logiciel et la confidentialité des données auxquelles l'administrateur accédera dans la stricte limite de ses besoins, l'administrateur devra prendre les précautions suivantes : information préalable de l'utilisateur et recueil de son accord pour donner la main à l'administrateur (validation d'un message d'information apparaissant sur son écran), traçabilité des opérations de maintenance par la tenue d'un registre des interventions et clause de confidentialité et règles de déontologie dans le cadre du contrat de travail des administrateurs. L'utilisation de ces logiciels à des fins strictes d'assistance utilisateur n'est pas soumise à déclaration auprès de la CNIL.

L'administrateur réseau exerce une mission de contrôle, notamment réalisée à partir de la conservation de données techniques appelées données de connexion ou données relatives au trafic (ex. : adresses URL visitées, adresse IP, limites d'accès au serveur proxy, pare-feu).

Les établissements scolaires offrant un accès à Internet à leurs apprenants sont soumis aux dispositions de l'article L. 34-1 du code des postes et des communications électroniques. Selon cet article, les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne ont l'obligation de conserver les données de connexion des personnes utilisatrices de leurs services. En tout état de cause, il convient de rappeler que cette disposition n'impose pas d'identifier les élèves par la tenue, par exemple, d'un fichier des utilisateurs.

Ce contrôle est légitime dès lors qu'il est réalisé de manière transparente, à savoir avec une parfaite information des utilisateurs. La rédaction d'une Charte d'utilisation des outils informatiques ou numériques est particulièrement utile pour rappeler les obligations mutuelles de l'établissement et de l'utilisateur, définir les modalités des contrôles qui peuvent être effectués et les sanctions auxquelles s'expose l'utilisateur s'il ne respecte pas les règles d'utilisation.

Il est recommandé que la direction de l'établissement informe ses personnels au sujet :

- de l'existence de procédures de contrôles quant à l'utilisation de la messagerie électronique ou d'Internet ; cette information peut être assurée par l'envoi à chaque agent d'un courrier électronique dans lequel doivent être rappelées les mentions « informatique et libertés ». Cette information peut être utilement complétée par voie d'affichage ;
- des procédures de surveillance et d'archivage mises en œuvre pour des raisons de sécurité des systèmes d'information (ex. : encombrement du réseau) ;
- de la durée de conservation des données dans le cas de mesures d'archivage ;
- de l'existence et la date de la consultation préalable des instances représentatives du personnel.

WEBOGRAPHIE

https://www.cnil.fr/sites/default/files/typo/document/CNIL_Guide_enseignement.pdf

https://asso-generationnumerique.fr/

https://www.educnum.fr/

http://espe.univ-lyon1.fr/droitsetobligations/

https://les-savanturiers.learningplanetinstitute.org/wp-content/uploads/2017/06/le-byod-ou-bring-your-own-device.pdf

FICHES MÉMENTO

NOTIONS ESSENTIELLES DU DROIT À LA PROTECTION DES DONNÉES PERSONNELLES

1- DÉFINITION D'UNE DONNÉE PERSONNELLE
2- DROIT D'ACCÈS, D'OPPOSITION, DE RECTIFICATION...

Sources **Educadroit - Manuel d'éducation au Droit Monde numérique : quels droits ?**

Lien https://educadroit.fr/sites/default/files/Manuel-Education-au-Droit-2020-chap11.pdf

MODÈLE DE DEMANDE D'AUTORISATION DE L'UTILISATION DE L'IMAGE D'UNE PERSONNE

PRÊT À L'EMPLOI, À CONTEXTUALISER

Sources **Ministère de l'économie, des finances et de la relance**
Accueil du portail APIE Propriété intellectuelle

Lien https://www.economie.gouv.fr/apie/publications-propriete-intellectuelle

LICENCES LIBRES

CREATIVE COMMONS, NC, ND...

Sources **Ministère de l'économie, des finances et de la relance**
Accueil du portail APIE Propriété intellectuelle

Lien https://www.economie.gouv.fr/files/files/directions_services/apie/propriete_intellectuelle/publications/Licences_libres-Creative_Commons.pdf

LES RÈGLES DE NETIQUETTE

BONNES PRATIQUES À L'USAGE DES COURRIERS ÉLECTRONIQUES ET DES FORUMS

Sources **Ministère chargé de l'Éducation nationale et centre innovation pédagogique du Quebec**

Lien https://primabord.eduscol.education.fr/qu-est-ce-que-la-netiquette

DROITS D'AUTEUR ET...

1- EXCEPTION DE COPIE PRIVÉE
2- EXCEPTION DE COURTE CITATION
3- EXEMPLE DE TRAVAUX RÉALISÉS PAR LES ÉLÈVES QUI PEUVENT ÊTRE PROTÉGÉS PAR LE DROIT D'AUTEUR

Sources **Guide de droit d'auteur**

3e édition – 2017, Sous la direction scientifique de A. Lucas, Professeur émérite, Université de Nantes

E. Bouchet-Le Mappian, Docteur en droit, Université de Nantes

S. Chatry, Maître de conférences, Université de Perpignan Via Domitia

S Le Cam, Maître de conférences, Université de Rennes 2

Mise à jour par S. Le Cam, Maître de conférences, Université de Rennes 2 et S.

Chatry, Maître de conférences, Université de Perpignan Via Domitia

Liens https://www.enssib.fr/bibliotheque-numerique/documents/67553-guide-de-droit-d-auteur.pdf

https://eduscol.education.fr/2992/comprendre-les-droits-d-auteur-avec-les-fiches-de-l-hadopi

LISTE DES ORGANISMES DE GESTION COLLECTIVE DES DROITS D'AUTEUR

ŒUVRES MUSICALES, GRAPHIQUES, AUDIOVISUELLES, LITTÉRAIRES

Sources **Ministère de l'économie, des finances et de la souveraineté industrielle et numérique**

Lien https://www.economie.gouv.fr/apie/propriete-intellectuelle-publications/conditions-utilisation-des-contenus-pas-affichees

MESSAGES LITIGIEUX SUR LES RÉSEAUX SOCIAUX

PAGES SPOTTED, JURISPRUDENCE, PRÉVENTION

Sources **Note DAJ A1 n° 13-122 du 22 avril 2013 parue dans la lettre d'information juridique du ministère de l'éducation nationale n° 176 de juin 2013**

Lien https://primabord.eduscol.education.fr/qu-est-ce-que-la-netiquette

Ce guide a été élaboré dans le cadre du plan d'action NumEA relatif au développement et à la valorisation du numérique éducatif dans l'enseignement technique agricole, par une équipe projet. Il s'appuie sur de nombreux textes et guides élaborés par d'autres institutions, avec une visée de contextualisation à l'enseignement agricole. Il est amené à évoluer régulièrement, sa version officielle sera hébergée sur le site ChloroFil.

NumEA
Numérique Éducatif
de l'Enseignement Agricole

Cheffe de projet NumEA
Nathalie HERAULT (DGER)

Groupe projet

Jean-Olivier SERRA (DGER)

Hélène LAXENAIRE (Institut-Agro-Florac)

Michel DUMAS (IEA)

Laurent VILLAIN (DRAAF - Nouvelle-Aquitaine et DPO)

Aurélie CANIZARES (ENSFEA)

Sylvie SOGNOS (ENSFEA)

Relecture

Nicolas BOIVIN (UNREP)

Thierry DEDIEU (CNEAP)

Merci infiniment aux professeurs des établissements relecteurs de ce guide.

Mise en page
L'institut Agro Enseignement à distance - 01N1-421

Crédit illustration
© strichfiguren.de - stock.adobe.com

Octobre 2023

UNREP
FORMER POUR REUSSIR

ENSFEA
Ecole Nationale Supérieure de Formation de l'Enseignement Agricole

CNEAP

MFR
CULTIVONS LES RÉUSSITES

L'INSTITUT agro Montpellier

L'INSTITUT agro Enseignement à distance

ENSEIGNEMENT AGRICOLE
L'AVENTURE DU VIVANT
RÉVÈLE TON TALENT