sciencespo.aix

Conseil d'administration
Institut d'Études Politiques d'Aix-en-Provence

DÉLIBÉRATION n° 2024-03-11-10

Le conseil d'administration, en sa séance du 11/03/2024,
sous la présidence de de Madame Aurélie Robineau-Israël,

Vu le Code de l'Éducation, notamment ses articles D. 741-9 à D. 741-11 ;
Vu le décret n°89-902 du 18 décembre 1989 relatif aux instituts d'études politiques dotés d'un statut d'établissement public administratif associés à une université ou à une communauté d'universités et établissements;
Vu la délibération n°2017/10/14-3 du conseil d'administration en sa séance du 14 octobre 2017 relative à la charte régissant l'usage des moyens numériques ;
Vu le règlement intérieur de l'institut d'études politiques d'Aix-en-Provence ;
Vu le règlement intérieur du Conseil d'administration ;

Considérant notamment les évolutions règlementaires intervenues depuis 2017, la charte régissant l'usage des moyens numériques de l'IEP et ses annexes approuvés par délibération n°2017/10/14-3 susvisée ont été renouvelés ;

DÉCIDE :

OBJET : Nouvelle charte régissant l'usage des moyens numériques et de ses annexes

Le conseil d'administration approuve la nouvelle charte régissant l'usage des moyens numériques de l'IEP ainsi que ses annexes (charte anti-plagiat, code de bonne conduite et corpus règlementaire) telles qu'annexées à la présente délibération.

Membres en exercice : 30
Quorum : 15
Présents et représentés : 26
Majorité des présents et représentés : 14

Cette délibération est adoptée par le conseil d'administration après en avoir délibéré et à l'issue d'un vote des membres par 26 voix POUR, 0 voix CONTRE et 0 abstention.

Fait à Aix-en-Provence, le 11/03/2024

Aurélie Robineau-Israël
Présidente du conseil d'administration
de l'IEP d'Aix-en-Provence

DATE AFFICHAGE ET PUBLICATION : 27/03/2024

Conseil d'administration
Lundi 11 mars 2024

CHARTE REGISSANT L'USAGE DES MOYENS NUMERIQUES DE SCIENCES PO AIX

Sommaire

ARTICLE I. CHAMP D'APPLICATION

La présente charte fixe les grands principes de l'usage des moyens numériques de Sciences Po Aix.

Le terme « moyens numériques » vise, dans la présente charte, tous les éléments ou toutes les ressources constituant le système d'information de Sciences Po Aix.
Ainsi, les moyens numériques représentent l'ensemble des logiciels et matériels, outils informatiques et services numériques, que Sciences Po Aix met à disposition des utilisateurs.

Les « utilisateurs », au sens de la présente charte, sont définis comme l'ensemble des personnes bénéficiant de l'autorisation d'accéder au système d'information de Sciences Po Aix.

Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent à Sciences Po Aix et à l'ensemble de ses utilisateurs.

Les utilisateurs ayant des fonctions d'administrateurs des moyens numériques sont soumis à une charte complémentaire et spécifique précisant leurs obligations particulières.

ARTICLE II. CONDITIONS D'UTILISATION DU SYSTEME D'INFORMATION ET DES MOYENS NUMERIQUES

Sciences Po Aix met à la disposition de ses utilisateurs un ensemble d'outils et de services numériques à des fins professionnelles.

L'usage des moyens numériques présente un caractère professionnel lorsqu'il intervient :

- dans le cadre des missions confiées par Sciences Po Aix, pour les utilisateurs membres de son personnel : enseignants, administratifs ou techniques, mais également ses prestataires et partenaires ;
- dans le cadre des activités pédagogiques, pour ses utilisateurs étudiants.

Par opposition, l'utilisation résiduelle à titre privé doit être non lucrative et raisonnable, tant dans sa fréquence que dans sa durée.

Cette utilisation ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service.

Toute information est dite professionnelle à l'exception des données explicitement désignées par l'utilisateur comme relevant de sa vie privée. Ainsi, il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu explicitement[1] à cet effet et en mentionnant le caractère privé sur la ressource[2]. La ressource pouvant être un message, un fichier, ou toute autre ressource numérique. La sauvegarde régulière de données à caractère privé incombe à l'utilisateur.

L'utilisation du système d'information à titre privé doit respecter les lois et la réglementation en vigueur. Conformément aux dispositions du code pénal, l'utilisation ne doit pas diffuser des informations ou données dont le contenu présente un caractère illégal, notamment raciste, diffamatoire ou injurieux. Ceci s'applique tant aux fichiers qu'aux messages avec ou sans pièces attachées quelle que soit la forme des contenus (textuels, sonores, audiovisuels ou multimédias)

La consultation de sites à caractère pornographique ou illicite depuis les locaux de l'institution est interdite.

[1] Pour exemple, cet espace pourrait être dénommé « _privé_ » ou «_Personnel_ »
[2] Pour exemple, « _privé_nom_de_l_objet_ » : l'objet pouvant être un message, un fichier ou toute autre ressource numérique

ARTICLE III. PRINCIPES DE SECURITE

Section 3.1 Gestion des mots de passe et accès aux ressources

Sciences Po Aix met en œuvre les mécanismes de protection appropriés sur les moyens numériques mis à la disposition des utilisateurs.

L'utilisateur est informé que les codes d'accès constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cependant, cette mesure ne confère pas aux outils informatiques protégés un caractère personnel.

Les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est conférée. La sécurité du système d'information mis à sa disposition lui impose :

- de respecter les consignes de sécurité, notamment les règles relatives à la gestion des codes d'accès ;
- de garder strictement confidentiels son (ou ses) codes d'accès et ne pas le(s) divulguer à un tiers ;
- de veiller au respect de la sécurité liée aux mots de passe permettant l'accès à son environnement de travail (logiciels métiers, messagerie électronique, etc.),
- de respecter la gestion des accès, en particulier ne pas utiliser les codes d'accès d'un autre utilisateur, ni chercher à les connaître.

Si, pour des raisons exceptionnelles et ponctuelles, un utilisateur se trouve dans l'obligation de communiquer son mot de passe, il devra procéder, dès que possible, au changement de ce dernier ou en demander la modification à l'administrateur. Le bénéficiaire de la communication du mot de passe ne peut quant à lui le communiquer à son tour à un tiers, ni l'utiliser en dehors de la circonstance exceptionnelle à l'origine de sa communication.

Les mots de passe doivent être constitués de 8 caractères alphanumériques au minimum, dont au moins un chiffre et un caractère spécial. Par ailleurs, chaque utilisateur doit :

- Eviter de choisir un mot de passe ayant un lien avec son environnement familier,
- Changer ses mots de passe selon une périodicité de 3 mois.
- Veiller à la confidentialité de ses mots de passe et notamment s'abstenir de l'écrire sur un support facilement accessible,
- Changer immédiatement son/ses mot(s) de passe en cas de doute sur sa/leur confidentialité.

La sécurité des ressources mises à la disposition de l'utilisateur nécessite également plusieurs précautions :

- *de la part de Sciences Po Aix :*

- veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées, en dehors des mesures d'organisation de la continuité du service mises en place par la hiérarchie ;
- limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité.

- *de la part de l'utilisateur :*

- s'interdire d'accéder ou de tenter d'accéder à des ressources du système d'information pour lesquelles il n'a pas reçu d'habilitation explicite ;
- ne pas connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés dans le cadre de la mission de l'utilisateur.

En particulier :

L'utilisation des ressources informatiques de Sciences Po Aix via la connexion d'un équipement privé et extérieur (tels qu'un ordinateur, un commutateur, un modem, une borne d'accès sans fil) sur le réseau est interdite par défaut, sauf autorisation de Sciences Po Aix.

Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Elles peuvent être retirées à tout moment et prennent fin lors de la cessation de l'activité professionnelle qui a justifié leur octroi.

- ne pas installer, télécharger ou utiliser sur le matériel de l'institution des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, qui ne proviennent pas de sites dignes de confiance, ou qui n'ont pas reçu l'autorisation de l'institution.
- se conformer aux dispositifs mis en place par l'institution pour lutter contre les virus et les attaques par programmes informatiques.
- assurer la protection de ses informations et plus particulièrement celles jugées comme sensibles au sens de la politique de sécurité du système d'information (PSSI). En particulier, l'utilisateur ne doit pas transporter sans protection (telle qu'un chiffrement) des données sensibles sur des supports non fiabilisés tels que, par exemple, ordinateurs portables, clés USB ou disques externes. Les supports qualifiés comme « informatique nomade » introduisent une vulnérabilité des ressources informatiques et comme tels doivent être soumis aux règles de sécurité de l'institution et à une utilisation conforme aux dispositions de la présente charte.
- en cas d'accès distant au système d'information, il convient de prendre toutes les précautions nécessaires à la non divulgation de son mot de passe et de ses données auxquelles il a accès, en cohérence avec la politique de sécurité du système d'information (PSSI).

Section 3.2 Devoirs de signalement et d'information

Sciences Po Aix porte à la connaissance de l'utilisateur tout élément susceptible de lui permettre d'apprécier le niveau de risque encouru dans l'utilisation du système d'information.

L'utilisateur avertit sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le système d'information. Il signale également à la personne qui en est responsable toute possibilité soudaine d'accès à une ressource qui ne correspond pas à son habilitation.

Section 3.3 Mesures de contrôle de la sécurité

L'utilisateur est informé :

- que pour effectuer la maintenance corrective, curative ou évolutive, Sciences Po Aix se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition ;
- qu'une maintenance à distance est précédée d'une information de l'utilisateur ;
- que toute information bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire sera isolée, le cas échéant supprimée ;
- que Sciences Po Aix peut prévoir des restrictions d'accès spécifiques à son organisation tels que certificats électroniques, cartes à puces ou d'authentification, filtrages d'accès sécurisé.

Sciences Po Aix informe l'utilisateur que le système d'information peut donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité ou

de détection des abus, dans le respect de la législation applicable (notamment la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et libertés).

Les personnels chargés des opérations de contrôle du système d'information sont soumis au secret professionnel.
Ils ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions dès lors que ces informations sont couvertes par le secret des correspondances ou identifiées comme telles. Celles-ci relèvent de la vie privée de l'utilisateur.

En revanche, ils doivent communiquer ces informations si elles mettent en cause le bon fonctionnement technique des applications et leur sécurité, ou si elles tombent dans le champ de l'article 40 du code de procédure pénale.

Section 3.4 Paramétrage des postes de travail et sécurité

a) Principes généraux

Le poste de travail de l'utilisateur constitue un outil qui doit être protégé des intrusions. A cet égard, il est conseillé :

- De paramétrer la mise en veille automatique de l'ordinateur avec demande du mot de passe pour sa réactivation après une période d'inactivité,
- D'effectuer systématiquement une déconnexion des serveurs réseaux et de clore les applications actives avant de quitter son poste de travail.

b) Dispositif de protection logicielle

Sciences Po Aix a doté tous ses postes de travail ainsi que son infrastructure d'hébergement d'une solution de sécurité logicielle comprenant un antivirus et un pare-feu applicatif.

Il est interdit de désactiver, d'altérer le fonctionnement ou de désinstaller ce dispositif en exécution de la stratégie de sécurité de Sciences Po Aix. Cette politique prévoit notamment une mise à jour régulière des bases de connaissances du logiciel.

Qu'est-ce qu'un anti-virus ?

Un anti-virus a pour mission de détecter et d'éliminer les programmes malveillants tels que les virus et autres malwares. Il analyse et protège en permanence l'ensemble des ressources en cours d'exécution sur un poste informatique, incluant le disque dur, les clés usb, la mémoire, etc.

Qu'est-ce qu'un pare-feu ?

Un pare-feu également appelé « firewall », analyse le trafic réseau et identifie les activités illicites en provenance ou à destination d'un poste informatique. Il assure la protection de l'utilisateur contre les vols de données, l'hameçonnage (phishing), la navigation sur des sites illicites, etc.

c) Mises à jour

Les logiciels comportent des défauts. Parmi ces défauts, certains portent atteinte à la sécurité : ils sont nommés « vulnérabilité ». Au quotidien de nombreuses vulnérabilités sont découvertes dans les systèmes d'exploitation et les logiciels équipant les matériels informatiques. Ces failles sont très rapidement exploitées par les pirates les plus expérimentés pour tenter de prendre le contrôle ou voler des informations sur les postes de travail et les serveurs.

Il est donc primordial d'appliquer systématiquement les mises à jour de sécurité au fur et à mesure de leur publication.

d) Sauvegarde des données

Sciences Po Aix organise une sauvegarde des données sur un ensemble de postes informatiques (notamment ceux connectés au réseau « administratif »).
Pour tous les autres, une sauvegarde régulière par chaque utilisateur est l'unique moyen de garantir la pérennité des données et de se prémunir contre les conséquences néfastes d'un problème technique, d'une attaque informatique ou d'un vol.
La sauvegarde doit être organisée sur tout type d'appareil utilisé à titre professionnel, du poste informatique fixe au matériel nomade.

e) Les périphériques de stockage

Les périphériques de stockage comme les clés USB, les disques durs externes, cartes mémoire – voire les téléphones portables offrant cette fonctionnalité – sont un vecteur de plus en plus utilisé pour infecter les postes de travail.

Un périphérique de stockage d'origine inconnue peut non seulement contenir des virus, mais également être configuré pour « aspirer » le contenu du poste de travail à l'insu de son propriétaire.

Il est donc conseillé de :

- Privilégier son propre périphérique de stockage pour un échange de données plutôt que d'utiliser un matériel d'origine inconnue,
- De manière générale, il est recommandé de séparer les usages entre les périphériques de stockage professionnels et privés.

ARTICLE IV. COMMUNICATION ELECTRONIQUE

La messagerie est un outil de travail destiné à des usages professionnels. Elle peut constituer, sous certaines conditions, le support d'une communication privée (voir infra)

Les messages électroniques permettent d'échanger principalement des informations à vocation professionnelle, liées à l'activité directe de Sciences Po Aix. **L'utilisateur doit adopter en toutes circonstances un comportement responsable et respectueux des dispositions contenues dans la présente charte.**

Section 4-1 Adresses électroniques

Sciences Po Aix s'engage à mettre à la disposition de l'utilisateur une boîte à lettres professionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques. L'utilisation de cette adresse nominative est ensuite de la responsabilité de l'utilisateur. L'aspect nominatif de l'adresse électronique constitue le simple prolongement de l'adresse administrative. Il ne retire en rien le caractère professionnel de la messagerie.

L'adresse électronique nominative est attribuée à un utilisateur qui peut autoriser, à son initiative et sous sa responsabilité, l'accès de tiers à sa boîte à lettres.

Par principe, l'adresse électronique attribuée par l'administration au personnel de Sciences Po Aix prend la forme : prénom.nom@sciencespo-aix.fr

L'adresse électronique attribuée par l'administration aux étudiants de Sciences Po Aix prend – sous réserve des cas d'homonymie – la forme : prénom.nom@etu.univ-amu.fr

Une adresse électronique, fonctionnelle, ou organisationnelle, peut être mise en place pour un utilisateur mais aussi pour un groupe d'utilisateurs pour les besoins de Sciences Po Aix.
La gestion d'adresses électroniques fonctionnelles correspond à des listes de diffusion institutionnelles, désignant un utilisateur unique, une catégorie ou un groupe d'utilisateurs, relève de la responsabilité exclusive de Sciences Po Aix : ces listes ne peuvent être utilisées sans autorisation explicite ou validation par un modérateur.

Section 4.2 - Caractéristiques et limitations de la messagerie électronique

.

a) Pièces jointes et envois volumineux

Parmi ses fonctionnalités, la messagerie électronique permet l'échange de fichiers en « pièces jointes ».

L'émission, comme la réception, de messages contenant des pièces jointes est limitée à un usage raisonnable de cette fonctionnalité. L'usage est raisonnable lorsque :

- la taille des fichiers joints, en émission ou réception, est limitée et compatible avec le bon fonctionnement du service messagerie ;
- la fonctionnalité est utilisée principalement à des fins professionnelles.
-

Pour prévenir les abus, les messages émis ou reçus font l'objet d'une limitation technique de non distribution. En cas de dépassement de la taille limite, le message est rejeté et l'émetteur reçoit un message de non distribution.

Pour les envois volumineux, l'utilisateur doit recourir aux solutions mis à sa disposition (AMU Box, FileSender de Renater).
Le recours à des systèmes gratuits en ligne type wetransfer est à proscrire car la confidentialité des données transmises est incertaine.

b) Les destinataires

L'envoi de message à un grand nombre de destinataires est à proscrire. Cette pratique provoque le ralentissement des serveurs de messagerie de l'établissement.
L'utilisateur s'assure de l'identité et de l'exactitude des adresses des destinataires des messages.

Il veille à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter les diffusions de messages en masse, l'encombrement inutile de la messagerie et par conséquent la dégradation du service.

Surtout, les prestataires externes de services de messagerie assimilent ces messages à des « pourriels » ou « spams » et, en conséquence, placent l'université sur une liste noire. Ceci entraîne le blocage, chez les prestataires, de tous les messages en provenance de Sciences Po Aix.

Pour prévenir de tels dysfonctionnements, une limite technique est mise en œuvre par la direction du Système d'Information et Stratégie Numérique : en cas d'abus, le compte de l'expéditeur est bloqué.
S'il est nécessaire de diffuser des messages à de très nombreux destinataires, il est impératif d'utiliser les listes de diffusion, qui ne provoquent aucunes perturbations.

c) Divers

Sont interdits les messages comportant des contenus à caractère illicite quelle qu'en soit la nature. Il s'agit notamment des contenus contraires aux dispositions de la loi sur la liberté d'expression ou portant atteinte à la vie privée d'autrui comme, par exemple, des atteintes à la tranquillité par la menace, des atteintes à l'honneur par la diffamation, l'injure non publique, la violation des droits d'auteurs, des atteintes à la protection des marques….

En cas de redirection des messages vers un autre serveur de messagerie, l'utilisateur doit veiller à garantir le caractère confidentiel des messages professionnels qu'il redirige. La redirection des messages est de la responsabilité des utilisateurs ainsi que sa mise à jour. Sciences Po Aix ne connaissant et n'assurant le bon fonctionnement que de l'adresse de messagerie qu'elle met à disposition.

Les messages électroniques échangés avec des tiers peuvent constituer une preuve ou un élément de preuve susceptible d'engager la responsabilité de l'établissement.
L'utilisateur doit, en conséquence, être vigilant sur la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels.

Section 4-3 Stockage et archivage des messages électroniques

L'utilisateur doit mettre en œuvre les moyens nécessaires à la conservation des messages qui pourraient être indispensables à son activité.
La messagerie des personnels de Sciences Po Aix est sauvegardée quotidiennement, ce qui ne dispense en aucun cas les utilisateurs de procéder à un archivage personnel.

Chaque utilisateur doit en conséquence organiser lui-même la conservation de ces éléments en décidant :

- du nombre de sauvegardes et de leur périodicité ;
- du choix des fichiers et messages conservés et de ceux qui sont détruits ;
- de la méthode et de la durée de stockage.

Il est aussi rappelé que dans le cadre de la règlementation sur la protection des données, la durée de conservation des données à caractère personnel est limitée en fonction de leur catégorie et de leur finalité. Cette règle s'applique aux données personnelles figurant dans la messagerie personnelles (corps des messages ou pièces jointes).

Par ailleurs la conservation de données personnelles dans sa messagerie n'est pas recommandée, le risque de pertes, vol ou fuites de ces données étant plus important.

L'utilisateur doit donc veiller à « nettoyer » régulièrement sa messagerie de toutes données à caractère personnel en supprimant les messages et pièces jointes concernés. Si la durée de conservation des données personnelles n'est pas achevée, les messages et fichiers joints sont alors enregistrés dans les dossiers concernés du poste de travail de l'utilisateur.

Section 4-4 - Sécurité anti-virale

Il est déconseillé d'ouvrir des fichiers en provenance d'un expéditeur inconnu, pièces jointes ou de cliquer sur un lien présent dans le message.
Cette prescription concerne en particulier les fichiers compressés ou exécutables dont l'ouverture peut notamment générer l'activation de virus informatique, de codes malveillants, susceptibles d'entraîner des conséquences d'une extrême gravité pour Sciences Po Aix.

Les utilisateurs sont informés que Sciences Po Aix se réserve le droit de retenir, d'isoler, et/ou de supprimer tout message à l'aide de moyens automatisés et ce, sans que ces messages aient été nécessairement ouverts, afin de vérifier qu'ils ne comportent pas de virus.

D'une manière générale les utilisateurs sont informés que tout message bloquant ou présentant une difficulté technique d'acheminement à son destinataire peut être détruit sur décision de la direction du Système d'Information et Stratégie Numérique.

ARTICLE V - INTERNET

Il est rappelé qu'Internet est soumis à l'ensemble des règles de droit en vigueur.

L'utilisation d'Internet (par extension Intranet) constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'accessibilité de l'information au sein et en dehors de Sciences Po Aix.

Sciences Po Aix met à la disposition de l'utilisateur un accès Internet chaque fois que cela est possible.

Internet est un outil de travail ouvert à des usages professionnels (administratifs et pédagogiques). Si une utilisation résiduelle privée, telle que définie peut-être tolérée, il est rappelé que les connexions établies grâce à l'outil informatique mis à disposition par l'administration sont présumés avoir un caractère professionnel. L'administration peut les rechercher aux seules fins de les identifier.

a) Sécurité

L'établissement se réserve le droit de filtrer ou d'interdire l'accès à certains sites.
L'accès général aux sites n'est autorisé qu'au travers des dispositifs mis en place par Sciences Po Aix. Des règles de sécurité supplémentaires peuvent être précisées, s'il y a lieu, dans un guide d'utilisation établi par le service ou Sciences Po Aix.

Les utilisateurs ne doivent recourir qu'aux navigateurs sélectionnés et qualifiés par le Direction du Système d'Information et Stratégie Numérique, en respectant ses préconisations sur leur paramétrage et en privilégiant les extensions (plugins et modules complémentaires) recommandées par Sciences Po Aix.

Certains sites malveillants profitent des failles des navigateurs pour récupérer les données présentes sur le poste de travail. D'autres sites mettent à disposition des logiciels qui, sous une apparence anodine, peuvent prendre le contrôle de l'ordinateur et transmettre son contenu à des tiers, à l'insu de son utilisateur.
Il convient de faire preuve de prudence, s'abstenir de se connecter à des sites suspects et éviter de télécharger des logiciels dont l'innocuité n'est pas garantie ; par exemple : vérifier la pérennité du logiciel et / ou la nature de l'éditeur.

Les utilisateurs sont invités à privilégier la navigation en mode « privé », option disponible sur tous les navigateurs proposés par la DSISN.
Ce mode limite le stockage des données de navigation. Il évite ainsi la conservation d'informations personnelles, dont les mots de passe, dans la mémoire du navigateur. Concrètement, il permet de supprimer les « témoins de connexion » ou « cookies », susceptibles d'engendrer des risques pour la sécurité des informations personnelles, notamment lorsque plusieurs utilisateurs ont accès au même poste.

b) Publication sur les sites Internet et Intranet de Sciences Po Aix

Toute publication de pages d'information sur les sites Internet et Intranet de Sciences Po Aix doit être validée par un responsable de service ou responsable de publication nommément désigné.

Aucune publication de pages d'information à caractère privé sur les ressources du système d'information de Sciences Po Aix n'est autorisée, sauf autorisations expresses ou dispositions particulières.

c) Téléchargements

Tout téléchargement de fichiers sur Internet, notamment de sons ou d'images, doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis à l'article VI, ou dans le cadre des contrats passés par Sciences Po Aix.

Sciences Po Aix se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité du système d'information tels que des virus pouvant altérer le bon fonctionnement du système d'information de Sciences Po Aix, les codes malveillants ou encore les programmes espions.

ARTICLE VI – MATERIEL NOMADE

Section 6-1 Principes généraux

Lorsqu'un équipement nomade, de type appareil photo numérique, caméscope, téléphone mobile, ordinateur portable ou tablette, est confié à un utilisateur de Sciences Po Aix, cette mise à disposition :

- est réputée intervenir dans le cadre exclusif des activités professionnelles du bénéficiaire ;
- entraine l'obligation pour le bénéficiaire d'apporter tous les soins nécessaires à la bonne conservation de ce matériel.

Par exemple, le bénéficiaire doit veiller particulièrement à :

- ne pas exposer l'équipement confié à la chaleur ni à l'humidité ;
- ne pas le laisser sans surveillance ;
- ranger le matériel non-utilisé dans un endroit sécurisé.

L'accès au réseau local est réservé au matériel confié par Sciences Po Aix, aucun autre matériel ne doit y être connecté.

Section 6-2 - Vol / Perte

En cas de vol de l'équipement confié, une déclaration doit être effectuée sans délai à la DSISN en premier et en second lieu au commissariat de police le plus proche. Une copie de cette déclaration devra être adressée à Sciences Po Aix.
Toute fausse déclaration est passible de sanctions disciplinaires et / ou de poursuites pénales.

Section 6-3 - Détérioration

En cas de détérioration du matériel nomade prêté, celui-ci doit être restitué à la DSISN avec un descriptif des dommages constatés et un exposé des circonstances à l'origine de la détérioration.

ARTICLE VII - DISPOSITIONS GENERALES

Section 7-1 – Respect de la propriété intellectuelle

a) Général

Sciences Po Aix rappelle que l'utilisation des ressources informatiques implique le respect de ses droits de la propriété intellectuelle ainsi que ceux de ses partenaires et plus généralement de tous tiers titulaires de tels droits.

En conséquence, chaque utilisateur doit :

- utiliser des logiciels dans les conditions des licences souscrites ;
- ne pas reproduire, copier, diffuser, modifier ou utiliser des logiciels, bases de données, pages web, textes, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

b) Anti-plagiat

Dans le cadre de sa démarche de mise en place d'outils de prévention et de détection du plagiat, Sciences Po Aix met à disposition de ses enseignants chercheurs un logiciel de détection de similitude.
Ce service permet d'analyser des travaux rendus par les étudiants sous forme numérique, pour repérer et identifier les paragraphes similaires à des textes disponibles en ligne ou dans les bibliothèques de référence et dont les sources ne seraient pas citées.

« Le plagiat consiste à :

- s'attribuer les propos, les productions ou les idées d'autrui, sans citer la source ou l'auteur ;
- s'approprier les contenus disponibles sur Internet en format textes, audio, vidéo, image, ou autre sans citer la source ou en paraphrasant de manière inadéquate. »

Sources : Université Laval, définition du plagiat. 2012, 30 mars. « Le plagiat : informer, sensibiliser et prévenir » [en ligne]. Date de consultation : septembre 2016

Légalement, le plagiat n'est pas un délit, mais la contrefaçon l'est, car on fait passer pour sien le travail d'autrui, et on le fait passer pour original.

Sciences Po Aix informe ses étudiants que leurs productions (rapport de stage, mémoire, thèse, etc…) sont susceptibles d'être analysées par la solution de détection de similitudes.
Les sanctions pouvant être prises à l'encontre des auteurs de plagiat sont notamment disciplinaires.

Section 7-2 – Protection des données personnelles

L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitement de données à caractère personnel, conformément au règlement européen relatif à la protection des données à caractère personnel dit « RGPD ».

Les données à caractère personnel sont des informations qui permettent, sous quelque forme que ce soit, directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent.

Toutes les créations de fichiers comprenant ce type d'informations et demandes de traitement afférent, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants, sont soumises aux formalités préalables prévues par la loi « Informatique et Libertés ».

En conséquence, tout utilisateur souhaitant procéder à une telle création devra en informer préalablement les services compétents (et le correspondant Informatique et Libertés qui sera désigné ultérieurement) qui prendront les mesures nécessaires au respect des dispositions légales.

Par ailleurs, conformément aux dispositions de cette loi, chaque utilisateur dispose d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation du système d'information. Ce droit s'exerce auprès du responsable hiérarchique du service ou de Sciences Po Aix dont il dépend.

ARTICLE VIII - GESTION DES ABSENCES ET DES DEPARTS

a) Préparer son départ

Aux fins d'assurer notamment la bonne continuité du service, l'utilisateur prépare son départ notamment en :

- Demandant la suppression des accès aux logiciels, application de travail (SIFAC, APOGEE, etc.)
- Communiquant ses accès à des outils, plateforme, etc. auxquels il serait le seul à accéder dans le cadre de ses missions (télérecours, Panopto, …) afin que son successeur ou tout autre collègue en charge de la continuité du service puisse y accéder. Les demandes seront ensuite effectuées pour reprendre les données sous un autre identifiant, mail et mot de passe.
- Rendant disponible sur le poste informatique mis à sa disposition par Sciences Po Aix tous les dossiers archivés et en cours
- Supprimant tout dossier personnel de son poste informatique
- S'assurant de la mise en place d'un message dans sa messagerie électronique informant de son départ et orientant les demandeurs vers un autre contact
- Demandant le retrait de son adresse électronique professionnelle des différentes listes de diffusion
- Triant sa messagerie notamment en transmettant à ses collègues compétents les correspondances liées à des dossiers en cours ou nécessaire à la continuité du service
- Enregistrant dans des dossiers accessibles les pièces jointes à certaines correspondances et qui doivent être conservées
- Vidant sa messagerie de toutes correspondances à caractère personnel

A noter

En cas d'absence, notamment si celle-ci est prolongée (maladie, vacances ou autres) ou affecte la continuité du service, le supérieur hiérarchique de **l'agent peut demander à avoir accès à son poste (y compris messagerie professionnelle)** et exiger la communication de ses identifiants et mots de passe.

Cet accès, exceptionnel et ponctuel, n'est toutefois possible que si les conditions cumulatives suivantes sont observées :

- Que le(s) information(s), document(s) ou message(s) justifiant l'accès soient indispensables à l'activité de l'établissement et que ce dernier ne dispose d'aucun autre moyen de se les procurer,
- Qu'une demande expresse et motivée soit formulée auprès de la directrice de la DSISN, après avis du secrétaire général.
- Que la consultation de l'ordinateur ou messagerie concernés se fasse exclusivement en présence de la directrice de la DSISN ou de son représentant.

La personne accédant ainsi à l'ordinateur s'engage expressément à **respecter la vie privée** de l'agent et la confidentialité de ses documents personnels. Elle ne pourra prendre connaissance d'un document clairement identifié comme personnel qu'après vous avoir invité à être présent ou en cas de risque particulier pour l'établissement.

En ce qui concerne la messagerie professionnelle, il est aussi rappelé, même si les messages personnels ne sont pas interdits, que tout message reçu ou envoyé depuis le poste de travail mis à disposition par Sciences Po Aix a par principe un caractère professionnel. Dans ce cas, il peut le consulter. Toutefois, si le message est clairement identifié comme étant personnel, par exemple, si l'objet du message précise clairement qu'il s'agit d'un message privé ou personnel, Sciences Po Aix n'en prendra pas connaissance en application du secret des correspondances.

b) Données professionnelles

L'utilisateur informe sa hiérarchie des modalités d'accès aux applications et données permettant d'assurer la continuité de service.
Les mesures de conservation des données professionnelles sont définies avec le responsable hiérarchique désigné au sein de Sciences Po Aix.

c) Données privées (ou « personnelles »)

L'utilisateur est responsable de son espace de données à caractère privé. Lors de son départ définitif du service ou de l'établissement, il lui appartient de détruire cet espace. La responsabilité de l'administration ne peut être engagée quant à la conservation de cet espace. Les procédures sont décrites dans le guide de l'utilisateur, annexé à la présente charte.

d) Fermeture du compte

Sciences Po Aix informe l'utilisateur de la date à laquelle son compte de messagerie électronique sera fermé afin de lui permettre de vider sa messagerie.
A l'issue de cette suppression l'adresse électronique nominative de l'utilisateur sera supprimée.

ARTICLE IX. ANNEXES ET DOCUMENTS COMPLEMENTAIRES A LA PRESENTE CHARTE

- Corpus documentaire et règlementaires (annexe)
- Code de bonne conduite informatique (document complémentaire)
- Charte anti-plagiat (document complémentaire)

La présente charte est annexée au règlement intérieur de Sciences Po Aix.

Pour en savoir plus

a) Ressources internes complémentaires

- Le guide de sensibilisation RGPD à l'usage du personnel
- La charte interne pour le respect des droits d'auteur
- La procédure relative aux droits d'auteurs et image

b) Liens utiles

- ANSSI (Agence Nationale de la Sécurité des Systèmes d'information) :*http://www.ssi.gouv.fr/*
- Portail de la Sécurité Informatique : *http://www.securite-informatique.gouv.fr/*

CERTA, Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques : *http://www.certa.ssi.gouv.fr/*

Assistance

En cas de besoin d'assistance ou de renseignements complémentaires, vous pouvez adresser vos demandes au support informatique de l'Institut d'Etudes Politiques d'Aix en Provence en écrivant à l'adresse suivante : informatique@sciencespo-aix.fr

Données personnelles

Pour toutes questions portant sur le traitement des données à caractère personnel ou pour exercer vos droits afférents à la protection de vos données personnelles, vous pouvez contacter le DPO de Sciences Po Aix à l'adresse suivante : delegue.protection-donnees@sciencespo-aix.fr

CHARTE ANTI-PLAGIAT A DESTINATION DES ETUDIANTS

Annexe 1 à la charte régissant l'usage des moyens numériques de Sciences Po Aix

Préambule

Le plagiat consiste en la réutilisation partielle ou totale d'une œuvre, sans accord de son auteur, et sans respect de son droit moral.

C'est le fait de « s'approprier la réflexion et l'analyse d'autrui sans en citer la source. » (*Université de Lausanne, UNIL 2003-2004 Histoire en pratique(s) : le plagiat*).

L'auteur jouit du droit au respect de son nom, de sa qualité et de son œuvre. Ce droit est attaché à sa personne. Il est perpétuel, inaliénable et imprescriptible (art. L.121-1 du CPI).

Une charte pour le respect des droits d'auteurs, éditée par Sciences Po Aix, rappelle les grands principes de la propriété intellectuelle et les droits et obligations des étudiants. Les étudiants doivent en prendre connaissance au moment de leur inscription sur la plateforme pédagogique de Sciences Po Aix.

Article 1 : Objet et domaine d'application

La présente charte a pour but de rappeler aux étudiants l'interdiction de plagier, les principes à respecter dans leurs travaux pour respecter les droits d'auteurs et éviter tout plagiat.

Elle rappelle également les sanctions auxquelles ils s'exposent en cas de plagiat.

Article 2 : Travaux des étudiants

4.1 Chaque travail demandé à l'étudiant doit être original, c'est à dire ne pas reprendre tout ou partie d'un travail similaire sans citation de l'auteur, ni autorisation de ce dernier si la réglementation l'exige.

4.2 Il reste possible à l'étudiant de s'appuyer sur des travaux déjà existants, si les sources sont dûment citées et les autorisations nécessaires accordées à l'étudiant.

4.3 La citation des sources permet à l'étudiant de valoriser son travail, et permet de vérifier l'exactitude de l'extrait cité. Les citations doivent se plier à des règles précises, à savoir :

- La citation doit être mise entre guillemet, ou en retrait par rapport au corps du texte, afin d'être identifiée clairement comme telle.
- Elle doit reproduire avec exactitude, aussi bien les mots que la ponctuation, et toutes les autres spécificités du texte d'origine.
- En cas de nécessité de modifier une citation, il est possible d'ajouter entre crochets la modification et/ou l'ajout à la citation.
- Toute citation doit voir ses sources renseignées,
- soit par un renvoi aux notes de bas de page, soit par un renvoi à la bibliographie rendue avec le travail.

4.4 En cas de manquement aux règles précédemment cités, le jury pourra catégoriser à sa discrétion la citation de l'étudiant comme un plagiat, et appliquer les sanctions qui s'imposent.

Article 3 : Contrôles en faveur de la lutte contre le plagiat

3.1 Sciences Po Aix s'est doté d'un logiciel anti-plagiat, permettant une analyse détaillée des productions des étudiants.

3.2 En déposant vos travaux sur une plateforme de Sciences Po Aix, vous donnez votre consentement pour l'analyse de vos documents, ainsi que l'ajout de ce dernier à notre base de documents.

Article 4 : Sanctions

5.2 Le plagiat est considéré comme une fraude, exposant son ou ses responsables à des sanctions disciplinaires par l'établissement dans les conditions prévues par le code de l'éducation (articles R. 811-11 et suivants)

Les sanctions disciplinaires pouvant être prises à l'encontre des responsables de plagiat (article R. 811-36 du code de l'éducation), peuvent aller de l'avertissement à l'exclusion définitive de tout établissement d'enseignement supérieur en passant par l'exclusion temporaire de Sciences Po Aix pour une durée pouvant aller jusqu'à 5 ans.

A noter : dès lors qu'une sanction est prononcée, **cela entraîne automatiquement la nullité de l'épreuve correspondante.**

La section disciplinaire de Sciences Po Aix pourra également décider de prononcer, en plus de la nullité de l'épreuve correspondante, la nullité du groupe d'épreuves ou de la session d'examen ou du concours.

5.2 Le plagiat peut être assimilé à de la contrefaçon et toute contrefaçon est un délit, exposant son ou ses responsables à des sanctions telles que le prévoit le code de la propriété intellectuelle (article L335-1 et suivants).

En cas de plagiat avéré ou de contrefaçon, la procédure disciplinaire ne préjuge pas d'éventuelles poursuites judiciaires exposant à des sanctions pénales.

CODE DE BONNE CONDUITE INFORMATIQUE

LES BONNES PRATIQUES

Annexe 2 à la charte régissant l'usage des moyens numériques de Sciences Po Aix

Le présent code de bonne conduite met en évidence de manière synthétique les risques informatiques et les moyens à mettre en œuvre par chaque utilisateur pour minimiser ces risques.

Chaque utilisateur[1] s'engage à :

- **Conserver confidentiellement les accès au réseau de Sciences Po Aix, et aux accès logiciels qu'il utilise,** il ne les communique à personne
- **N'enregistrer que des informations professionnelles appartenant à Sciences Po Aix,** sur le réseau interne de Sciences Po Aix
- **Bien distinguer les données personnelles qui lui appartiennent,** des données professionnelles, qui appartiennent exclusivement à Sciences Po Aix
- **S'assurer que les données professionnelles sont stockées de manière à faire l'objet d'une sauvegarde,** pour ne pas être tenue responsable d'une perte de données. L'utilisateur ne stocke donc pas sur un disque dur externe ou une clé USB.
- **Classifier ses données strictement personnelles dans un fichier intitulé « Personnel »** car tous les autres messages, fichiers ou dossiers sont présumés être professionnels et consultables par son supérieur hiérarchique.
- **Consulter des sites internet pour son usage personnel de manière** exceptionnelle et ne portant pas atteinte aux bonnes mœurs ou présentant un risque (jeux en ligne, streaming ou site de rencontre, etc.) car l'utilisateur sait que le réseau internet de Sciences Po Aix est à vocation professionnelle.
- **Ne pas utiliser les outils informatiques de Sciences Po Aix,** pour :
    - Diffuser des informations confidentielles relatives à Sciences Po Aix, ses agents, ses étudiants, ses enseignants, ses partenaires et ses sous-traitants,
    - Télécharger, stocker, utiliser des programmes, logiciels ou données protégées par les droits de la propriété intellectuelle, sauf à disposer des autorisations nécessaires,
    - Stocker, consulter, envoyer ou recevoir de manière délibérée sur son ordinateur des logiciels, programmes, fichiers, vidéos, images ou messages dont le contenu est susceptible d'être illégal ou d'être contraire à l'ordre public, aux bonnes mœurs ou de porter atteinte à la dignité d'autrui,
    - Effectuer une copie d'un logiciel mis à disposition, y compris à des fins de sauvegarde, sans autorisation expresse et préalable de la direction informatique,
    - Modifier les moyens informatiques mis à disposition, notamment par modification des paramétrages, sans autorisation expresse et préalable de la direction informatique,
    - Procéder à du harcèlement, des menaces ou des injures,
    - Plus généralement, d'utiliser les ressources mises à disposition par Sciences Po Aix dans le cadre d'une activité illégale, quelle qu'elle soit.
- **Ne pas s'inscrire sur un réseau social avec ses coordonnées professionnelles** sans accord préalable de la direction.
- **A avoir un bon usage des médias sociaux** car l'utilisateur a conscience qu'une utilisation inappropriée peut porter atteinte à sa vie privée, à celle des autres utilisateurs, et engendrer des dommages à la réputation de Sciences Po Aix, ses agents, ses enseignants, ses étudiants, ses partenaires et de ses prestataires.

[1] Sont utilisateurs toutes les personnes bénéficiant de l'autorisation d'accéder au système d'information de Sciences Po Aix

- **Ne pas mettre de photos prises dans le cadre professionnel**, sur les réseaux sociaux, sauf sur demande explicite de Sciences Po Aix, ou avec son autorisation.
- **Faire les mises à jour de l'ordinateur et du téléphone professionnel** régulièrement (système, pilotes & logiciels) pour combler les failles de sécurité, en plus de pouvoir bénéficier éventuellement de nouvelles fonctionnalités.
- **Vérifier l'authenticité d'un message suspect** auprès de l'expéditeur via un autre canal (Téléphone, SMS, etc.) avant d'ouvrir une pièce jointe (en particulier les fichiers de type fausses factures, ou en .exe qui sont en fait des applications) ou de cliquer sur un lien dans le message (il vaut mieux faire une recherche du site directement dans votre moteur de recherche).
- **Vérifier que la liste des destinataires n'est pas suspecte** à ses yeux.
- **Faire particulièrement attention aux messages écrits en anglais ou mal traduits**. En cas de doute, l'utilisateur supprime le message sans le transférer.
- **Éviter de faire suivre les « chaines »** afin de ne pas diffuser son adresse inutilement.
- **Privilégier le champ CCI (et non CC)** s'il a plusieurs envois à faire pour ne pas divulguer ses coordonnés à des contacts qui ne se connaissent pas
- **Tenir à jour son carnet d'adresses** en supprimant les contacts obsolètes régulièrement.
- **N'utiliser que des moteurs de recherche** connus et fiables tels que : Google, Bing, Exalead
- **Ne pas utiliser de clés USB sans en connaitre la provenance** et de s'être assuré de la fiabilité de son utilisateur
- **N'installer que des logiciels utiles,** téléchargés à partir des sites officiels (http://offurl.fr/ peut vous guider), tout en faisant attention à décocher toute demande d'ajout de logiciels tiers et/ou toolbar qui sont sélectionnés par défaut.
  - Ces dernières peuvent automatiquement remplacer mon moteur de recherche défini par défaut.
- **Éviter l'usage des assistants vocaux** intégrés qui augmentent sensiblement la surface d'attaque du terminal.
- **Limiter les inscriptions sur des sites Internet** et sécuriser ses mots de passe :
  - 8 caractères minimum dont au moins une Majuscule, minuscules, chiffres & caractères spéciaux
  - Changer régulièrement mon mot de passe tous les 3 mois environ et en avoir un différent par site. Ne pas les écrire sur un support facilement accessible et/ou non sécurisé
- **Faire attention aux données diffusées** sur internet, notamment sur les réseaux sociaux (Facebook, Twitter, et tous les autres...) ainsi que dans le Cloud.
- **Ne jamais divulguer ses habitudes à un inconnu** (départ de vacances, critères physiques) lors de ses échanges sur internet (réseaux sociaux, tchat, messagerie) afin d'éviter les attaques personnelles, cambriolages, etc.
- **Privilégier le partage de connexion sur un téléphone mobile de confiance** plutôt que de se connecter à un réseau Wifi (HotSpot, Connexion Publique, Hôtel, Restaurant, …)
- **Désactiver systématiquement le WiFi et le BlueTooth** de ses appareils quand il n'en n'a pas besoin.
- **Changer systématiquement les codes de déverrouillage** par défaut sur ses téléphones, tablettes, etc.
- **S'assurer que le site internet qu'il visite est certifié « https »** avant de mettre en ligne des données sensibles, et effectuer des achats en ligne.
- **Consulter le site « FIA-NET.com »** pour consulter l'indice de confiance d'un site marchand.
- **Prendre le temps de bien lire les messages d'avertissements** des systèmes, applications et sites internet, avant d'exécuter un programme ou d'ouvrir un fichier.
  - Ne pas ouvrir en cas de doute
- **En cas d'infection ou attaque, déconnecter mon matériel** du WiFi ou du réseau sans l'éteindre tant qu'il n'aura pas été étudié par le service informatique.
- **Informer le service informatique, de toute activité ou message suspect** dans sa messagerie ou sur son ordinateur
- **Avoir le réflexe de protéger ses données personnelles et ma vie privée**, ainsi que toutes les données personnelles portées à sa connaissance, et qui ne lui appartiennent pas.

CORPUS REGLEMENTAIRE

Annexe 3 à la charte régissant l'usage des moyens numériques de Sciences Po Aix

1. Préambule

Le présent document est une annexe à la charte régissant l'usage du système d'information et des moyens numériques par les personnels et étudiants de Sciences Po Aix. Il s'inscrit dans le prolongement de cette charte et autres documents qui y sont annexés (code de bonne conduite et charte anti-plagiat).

2. La protection des Systèmes d'Information

Les articles 323-1 et suivants du Code pénal prévoient les sanctions (emprisonnement d'une durée variable en fonction du délit et/ou une amende) susceptibles d'être prononcées en cas d'atteintes aux Systèmes de traitements automatisés.

Parmi les atteintes, rappelées par le code pénal, à un système d'information on peut citer (liste non exhaustive) l'introduction dans un système d'information sans y être autorisée, L'entrave du système, c'est-à-dire toute perturbation volontaire du fonctionnement d'un système informatique ou encore l'altération des données, c'est-à-dire toute suppression, modification ou introduction de données pirates, avec la volonté de modifier l'état du système informatique les exploitant.

3. La responsabilité en matière de transmission des informations

Les moyens informatiques mis à la disposition de l'utilisateur permettent l'accès à une communication et à une information importante et mutualisée. Or, de tels moyens de communication ne doivent pas permettre de véhiculer n'importe quelle information ou donnée.

Ainsi la transmission de messages, documents, images par quelque moyen que ce soit et quel que soit le support, à caractère violent, raciste, pornographique, terroriste, dégradant ou de nature à porter gravement atteinte à la dignité humaine est pénalement sanctionnée par des peines d'emprisonnement et d'amendes (articles 227-23 et 227-24 du Code pénal).

4. La protection des droits de propriété intellectuelle

Cette partie sur la propriété intellectuelle est spécifique aux usages numériques. Elle est complémentaire à la charte pour le respecte des droits d'auteurs en ligne sur le site de Sciences Po Aix et à la procédure interne relative aux droits d'auteur et à l'image mise à la disposition des personnels.

a. Les règles de protection du droit d'auteur

En vertu des règles du **Code de la propriété intellectuelle** (CPI) :« *L'auteur d'une œuvre de l'esprit jouit sur cette œuvre du seul fait de sa création d'un droit de propriété incorporel et exclusif opposable à tous* » (article L111-1 du CPI).

Cette disposition s'applique à toutes les œuvres de l'esprit, dès lors qu'elles présentent une certaine originalité, quel que soit le genre, la forme d'expression, le mérite ou la destination.

Sont notamment considérées comme des œuvres de l'esprit, au sens du Code de la propriété intellectuelle et en particulier de l'article L.112-2, les œuvres suivantes :

- Les livres, brochures et autres écrits littéraires, artistiques et scientifiques.
- Les conférences, allocutions et autres œuvres de même nature.

- Les œuvres dramatiques ou dramatico-musicales.
- Les œuvres chorégraphiques.
- Les œuvres musicales avec ou sans paroles.
- Les œuvres cinématographiques et autres œuvres consistant dans des séquences animées d'images sonorisées ou non, dénommées ensembles œuvres audiovisuelles.
- Les œuvres de dessins, de peintures, d'architectures, de sculptures, de gravures, de lithographies.
- Les œuvres graphiques et typographiques.
- Les œuvres photographiques et celles réalisées à l'aide de techniques analogues à la photographie.
- Les œuvres d'art appliqué.
- Les illustrations et les cartes géographiques.
- Les logiciels, y compris le matériel de conception préparatoire.

Les actes de reproduction en tout ou partie, par tout moyen et sous toute forme sont ainsi soumis à l'autorisation du / ou des titulaire(s) des droits sur les œuvres. L'utilisation de ces œuvres suppose donc une acceptation préalable du / ou des titulaire(s) des droits. L'utilisateur est donc informé qu'à défaut d'une autorisation expresse du / ou des titulaire(s) respectant les dispositions du Code de la propriété intellectuelle, il lui est interdit d'utiliser une telle œuvre. À défaut, sa responsabilité civile et / ou pénale peut être engagée.

D'une manière générale, la difficulté à connaître précisément l'origine des données et donc les droits y afférents, en particulier avec le développement des moyens d'échanges d'informations en réseau ouvert comme Internet, oblige l'utilisateur à la plus grande prudence.

b. Les règles de protection des logiciels

Les logiciels sont protégés par le droit d'auteur. Toute reproduction, adaptation et / ou distribution du logiciel n'est autorisée que sous réserve du consentement du titulaire des droits sur ledit logiciel.

L'étendue et les caractéristiques des droits conférés sont définies en général par des contrats de licence d'utilisation qui précisent les modalités selon lesquelles est autorisée l'utilisation des logiciels visés.

L'utilisation du logiciel, même à des fins d'essais, de démonstration de courte durée ou à des fins pédagogiques et à défaut d'autorisation expresse et écrite du titulaire des droits est en principe interdite.

L'utilisateur d'un logiciel s'expose à des sanctions civiles et pénales prévues et réprimées par le Code de la propriété intellectuelle lorsqu'il utilise un logiciel sans autorisation.

Afin de prévenir les risques liés à la contrefaçon de logiciel, une vigilance particulière de l'utilisateur comme de son autorité hiérarchique est indispensable.

Est un délit de contrefaçon puni par le Code de la propriété intellectuelle (article L.335- 3 du Code de la propriété intellectuelle) « *toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur* », mais aussi la violation de l'un des droits de l'auteur d'un logiciel.

c. Les règles de protection des bases de données

On entend par « bases de données » un recueil d'œuvres de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen.

Les bases de données sont protégées par le Code de la propriété intellectuelle indépendamment de la protection dont peuvent bénéficier les données au titre du droit d'auteur contenu dans ladite base.

Les bases de données qui, par le choix ou les dispositions des matières, constituent des créations intellectuelles, bénéficient des dispositions du Code de la propriété intellectuelle.

L'utilisateur est susceptible de se rendre coupable de contrefaçon dans plusieurs cas :

- Lorsqu'il procède à toute extraction par transfert permanent ou temporaire de la totalité ou en partie, qualitativement ou quantitativement substantielle, du contenu d'une base de données sur un autre support, par tout moyen et sous toute forme que ce soit.
- D'autre part, par la réutilisation ou par la mise à disposition de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu de la base quelle que soit sa forme. À ce titre, un utilisateur des bases de données de l'Institut d'Etudes Politiques d'Aix-en-Provence ne saurait s'autoriser à utiliser à des fins privées par exemple un fichier d'adresses, dont l'Institut d'Etudes Politiques d'Aix-en-Provence est propriétaire, et ne saurait le télécharger ou en faire toute utilisation contraire au Code de la propriété intellectuelle.

5. La protection des marques

Le Code de la propriété intellectuelle protège la marque : « La marque de *fabrique, de commerce ou de service est un signe susceptible de représentation graphique servant à distinguer les produits ou services d'une personne physique ou morale* » (article L.711-1 du CPI).

Peuvent être définis et utilisés à titre de marque, tous signes nominaux, figuratifs ou sonores, tels que les mots, assemblages de mots, noms patronymiques, noms géographiques, pseudonymes, lettres, chiffres, sigles, emblèmes, photographies, dessins, empreintes, logos ou la combinaison de certains d'entre eux.

Ces droits et leur protection sur une marque confèrent à son titulaire, par un enregistrement, un droit de propriété sur cette marque. L'utilisateur ne peut, sauf autorisation du propriétaire, reproduire, utiliser ou apposer une marque, ainsi utiliser une marque protégée ainsi que de supprimer ou modifier une marque régulièrement déposée.

L'utilisateur s'interdit donc, sauf autorisation expresse du propriétaire, toute reproduction, usage ou apposition d'une marque ainsi que l'usage d'une marque reproduite pour des produits ou services identiques à ceux désignés dans l'enregistrement, la suppression ou la modification d'une marque.

L'utilisateur ne saurait utiliser une marque sur laquelle l'Institut d'Etudes Politiques d'Aix-en-Provence ne détient pas l'autorisation expresse d'utilisation dans le cadre de ses fonctions. Il lui sera en outre interdit d'utiliser à des fins privées toute marque dont l'Institut d'Etudes Politiques d'Aix-en-Provence est titulaire.

6. Le respect de la vie privée

a. Le droit à la vie privée

Le principe est posé par l'article 9 du Code civil qui prévoit que « *Chacun a droit au respect de sa vie privée. Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestres ou autres, propres à empêcher ou à faire cesser une atteinte à l'intimité de la vie privée.* »

b. Le secret des correspondances

Le secret des correspondances fait partie d'un des droits de la personne ainsi les atteintes aux droits de la personne en matière de secret des correspondances sont pénalement sanctionnées par de l'emprisonnement et une amende (article 226-15 du Code pénal).

Par ailleurs la violation du secret des correspondances par des personnes exerçant une fonction publique est considérée comme une atteinte à l'administration publique également sanctionnée par une peine d'emprisonnement et une amende (article 432-9 du Code pénal).

c. Le droit à l'image

L'utilisateur est informé qu'est puni d'un an d'emprisonnement et de 45 000 euros d'amende, « *Le fait au moyen d'un procédé quelconque, de porter volontairement atteinte à l'intimité de la vie privée d'autrui :*

- En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel.

- En fixant, enregistrant ou transmettant sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé. Lorsque les actes mentionnés ci-dessus ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé ». (Article 226-1 du Code pénal).

L'utilisateur est également informé qu'est puni d'un an d'emprisonnement et de 15 000 euros d'amende le fait de publier, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention (article 226-8 du Code pénal).