CHARTE D'UTILISATION DES SYSTEMES D'INFORMATION DE L'ECOLE CENTRALE DE LYON
V.2018 APPROUVEE PAR LE CA DU 18/10/2018

Etant entendu que la présente charte est adossée au règlement intérieur et ne saurait en être dissociée
L'Ecole Centrale de Lyon ci-après dénommée ECL

Préambule

Par "système d'information" s'entend l'ensemble des moyens matériels, logiciels, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition de l'«utilisateur».

L'informatique nomade tels que les assistants personnels, les ordinateurs portables, les téléphones portable est également un des éléments constitutifs du système d'information.

Par «utilisateur», s'entend toute personne physique ayant accès, dans le cadre de l'exercice de son activité, aux ressources du système d'information quel que soit son statut.

Par «données professionnelles » s'entend l'ensemble des données, des fichiers, des traitements gérés par l'établissement au sein de son activité quelle soit de recherche, d'enseignement, administrative ou culturelle.

Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires qui s'imposent et notamment, la sécurité, la performance des traitements et la conservation des données professionnelles.
(*) Rappel non exhaustif, des principales lois en dernière page.
La présente charte définit les règles d'usages et de sécurité que l'institution et l'utilisateur s'engagent à respecter : elle précise les droits et devoirs de chacun.

L'ECL porte à la connaissance de l'utilisateur la présente charte.

Considérant les engagements de l'ECL :

Les ressources mises à disposition dans l'établissement sont prioritairement à usage d'enseignement, de recherche, culturel et professionnel. Toutefois l'ECL est tenue de respecter la vie privée de chacun.

Considérant les engagements de l'utilisateur :

L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès.
Il a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède. Cette obligation implique le respect des règles d'éthique et de déontologie.

Les utilisateurs ont une responsabilité particulière dans l'utilisation qu'ils font des ressources mises à leur disposition par l'institution.
L'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat.
Il est arrêté ce qui suit :

ARTICLE I. CHAMP D'APPLICATION

Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent à l'établissement ainsi qu'à l'ensemble des utilisateurs.

ARTICLE II. CONDITIONS D'UTILISATION DES SYSTEMES D'INFORMATION

Section II.1 Utilisation et vie privée

Dans le cadre de son activité, les *systèmes d'information* sont mis à la disposition de l'utilisateur.

L'utilisation à des fins privées doit être non lucrative et raisonnable quantitativement, tant dans la fréquence que dans la durée. Elle ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service.

En toute hypothèse, le surcoût qui résulte de l'utilisation privée résiduelle des systèmes d'information doit demeurer négligeable au regard du coût global d'exploitation.

Toute information est réputée professionnelle à l'exclusion 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 à cet effet. Cet espace devra être dénommé « privé-personnel ». Le stockage et la sauvegarde des données à caractère privé incomberont à l'utilisateur.

Section II.2 Continuité de service : gestion des absences et des départs

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 son espace de données à caractère privé, la responsabilité de l'administration ne pouvant être engagée quant à la conservation de cet espace. Les mesures de conservation des données professionnelles sont définies avec le responsable ou les responsables désignés au sein de l'institution ou des structures dont dépend l'utilisateur.

ARTICLE III. PRINCIPES DE SECURITE

Section III.1 Règles de sécurité applicables

L'institution, son ministère de tutelle, ses fournisseurs d'accès et ses partenaires techniques extérieurs mettent en œuvre les mécanismes de protection appropriés sur les systèmes d'information mis à la disposition des utilisateurs.

L'utilisateur est informé que les mots de passe, les moyens d'accès (ou tout autre système d'authentification) constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. 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 des systèmes d'information mis à sa disposition lui impose de respecter les consignes de sécurité, les règles relatives à la gestion des mots de passe; notamment :

- de choisir un mot de passe sûr, n'ayant aucun lien avec l'environnement familier de l'«utilisateur» ;
- de choisir des mots de passe d'une complexité suffisante et de ne pas réutiliser les mêmes mots de passe sur des systèmes différents
- de changer de mot de passe régulièrement, si les applications le permettent ;
- de ne pas écrire son mot de passe sur un support facilement accessible ;
- de garder strictement confidentiel son (ou ses) mot(s) de passe et ne pas le(s) dévoiler à un tiers; En cas de doute sur cette confidentialité, il incombe à l'utilisateur de changer immédiatement ses mots de passe et d'en avertir la DSI;
- de respecter la gestion des accès, en particulier ne pas utiliser les noms et mots de passe d'un autre utilisateur, ni chercher à les connaître.
- L'utilisateur est responsable des opérations effectuées grâce à son identifiant et son mot de passe;

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisateur nécessite plusieurs précautions :

- de la part de l'institution :
    - veiller à ce que les ressources sensibles ne soient pas accessibles en cas d'absence (en dehors des mesures de continuité 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 :
    - Dans un cadre professionnel, les utilisateurs doivent utiliser les services numériques mis à disposition par l'École Centrale de Lyon, ses laboratoires ou partenaires cocontractants (mail, partage de fichier, plateforme de travail collaboratif …) et non des outils fournis par un prestataire extérieur (gratuit ou non) qui peuvent exposer de façon incontrôlée des informations sensibles à l'extérieur.
    - Si l'utilisateur ne bénéficie pas d'une habilitation explicite, il doit s'interdire d'accéder ou tenter d'accéder à des ressources du système d'information, même si cet accès est techniquement possible ;
    - ne pas connecter directement aux réseaux des matériels non confiés ou non autorisés par l'établissement ; par extension activer des points d'accès sans fil ou interagissant avec l'espace hertzien de l'établissement.
    - ne pas installer, télécharger ou utiliser sur le matériel de l'établissement, de logiciels ou progiciels sans autorisation explicite ;
    - appliquer les consignes de la DSI afin de s'assurer notamment que la configuration de son équipement suit les bonnes pratiques de sécurité (application des correctifs de sécurité, chiffrement, antivirus, etc.)

Section III.2 Devoirs de signalement et d'information

L'utilisateur doit avertir sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté, de toute perte, de tout vol ou de toute anomalie découverte telle une intrusion dans le système d'information, etc. : il signale également à la personne responsable du site toute possibilité d'accès à une ressource qui ne corresponde pas à son habilitation.

Section III.3 Mesures de contrôle de la sécurité

L'utilisateur est informé :

- que pour effectuer la maintenance corrective, curative ou évolutive, l'établissement 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 ou présentant une difficulté technique d'acheminement à son destinataire, peut être isolée, le cas échéant supprimée (information de type virus, logiciel espion, pourriel ou spam).
- que le système d'information peut donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus.

Section III.4 Obligations des personnes en charge de l'administration des Systèmes d'Information

Les personnels en charge de l'administration des Systèmes d'Information sont soumis au secret professionnel. Ils ne peuvent donc divulguer les informations qu'ils sont amenés à connaître dans le cadre de leur fonction en particulier lorsque ces informations sont couvertes par les secrets des correspondances ou relèvent de la vie privée de l'utilisateur dés lors que ces informations ne remettent pas en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt du service. Par ailleurs, les personnels en charge des Systèmes d'Information sont également soumis à la loi et ne peuvent pas diffuser d'information à leur hiérarchie sauf cas de plainte auprès du procureur de la république.

ARTICLE IV. COMMUNICATIONS ELECTRONIQUES

Section IV.1 Messagerie électronique

L'utilisation de la messagerie constitue l'un des éléments essentiels d'optimisation du travail et de mutualisation de l'information au sein de l'établissement.

(a) Adresses électroniques

L'établissement s'engage à mettre à la disposition de l'utilisateur une boîte à lettres nominative lui permettant d'émettre et de recevoir des messages électroniques.

L'adresse électronique nominative est attribuée à un utilisateur. Par norme sous la forme prenom.nom@(XXX.)ec-lyon.fr sauf cas d'homonymie.

Une adresse électronique, fonctionnelle ou organisationnelle, peut être mise en place si elle est exploitée par un service ou un groupe d'utilisateurs.

La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles, désignant une structure institutionnelle ou un groupe d'utilisateurs, relève de la responsabilité exclusive de l'ECL : ces adresses ne peuvent être utilisées sans autorisation explicite.

(b) Contenu des messages électroniques

Les messages électroniques permettent d'échanger principalement des informations à vocation liées à l'activité directe de l'ECL. En toutes circonstances, l'utilisateur doit adopter un comportement responsable et respectueux des dispositions contenues dans la présente charte.

Tout message sera réputé lié a l'institution sauf s'il comporte une mention particulière et explicite indiquant son caractère privé ou s'il est stocké dans un espace privé de données. Le sujet de la correspondance électronique devra commencer par la mention «privé-personnel».

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place.

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.

(c) Émission et réception des messages

L'utilisateur doit veiller 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 ainsi qu'une dégradation du service.
Il est interdit de diffuser des messages à un groupe de personnes dès lors qu'il existe une liste de diffusion institutionnelle dédiée pour cet usage.

(d) Statut et valeur juridique des messages

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles[6] 13691 et 136911 du code civil.
L'utilisateur doit en conséquence, être vigilant sur la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels.

(e) Stockage et archivage des messages

Chaque utilisateur doit organiser et mettre en oeuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve.
À ce titre, il doit notamment se conformer aux règles définies dans la présente charte.

Section IV.2 Internet

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

L'utilisation de la technologie 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 l'ECL

L'ECL met à la disposition de l'utilisateur un accès Internet chaque fois que cela est possible.
Le réseau de l'ECL est destiné à véhiculer le trafic engendré par des activités : d'enseignement, recherche, développements techniques, transfert de technologies, diffusion d'informations scientifiques, techniques et culturelles, expérimentations de nouveaux services présentant un caractère d'innovation technique.
A ce titre, tout accès à des tiers non autorisés à titre commercial ou non, rémunéré ou non, ou à des fins ludiques personnelles est interdit.

Internet est un outil de travail ouvert à des usages professionnels (administratifs, pédagogiques, recherches ou culturels) : il peut constituer le support d'une communication privée telle que définie en section II.1 dans le respect de la législation en vigueur. En complément de ces dispositions légales et au regard de la mission éducative de l'établissement, la consultation volontaire de contenus illicites depuis les locaux de l'établissement, est proscrite.

L'établissement se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder au contrôle a priori ou a posteriori des sites visités et des durées d'accès correspondantes.

L'établissement, son ministère de tutelle, ses fournisseurs d'accès ou ses partenaires techniques extérieurs se réservent le droit d'interdire certains accès, protocoles de communication, programmes ou modules pouvant porter atteinte à la sécurité.

Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'établissement

L'utilisateur est informé des risques et limites inhérents à l'utilisation d'Internet par le biais d'actions de formations ou de campagnes de sensibilisation.

Section IV.3 Téléchargements

Tout téléchargement de fichiers, notamment de sons ou d'images, sur le réseau Internet doit s'effectuer dans le respect des droits de la propriété intellectuelle.

L'établissement se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information (virus susceptibles d'altérer le bon fonctionnement du système d'information de l'établissement, code malicieux, programmes espions …).

ARTICLE V. TRAÇABILITE

L'établissement est dans l'obligation légale de mettre en place un système de journalisation, archivage des accès Internet, de la messagerie et des communications numériques échangées. Il est tenu de recueillir et conserver des informations sur les utilisateurs et peut, dans le cadre d'une enquête judiciaire, être dans l'obligation de les fournir aux autorités compétentes.

ARTICLE VI. RESPECT DE LA PROPRIETE INTELLECTUELLE

L'établissement rappelle que l'utilisation des moyens informatiques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et plus généralement, de tous tiers titulaires de tels droits.

En conséquence, chaque utilisateur doit :

- utiliser les logiciels dans les conditions des licences souscrites ;
- ne pas reproduire, copier, diffuser, modifier ou utiliser les 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.

ARTICLE VII. RESPECT DE LA LOI INFORMATIQUE ET LIBERTES ET DU REGLEMENT GENERAL DE PROTECTION DES DONNEES

L'utilisateur est informé que l'ECL se doit de respecter l'ensemble du corpus juridique applicable en matière de traitement automatisé de données à caractère personnel, au premier rang desquels les lois n° 7817 du 6 janvier 1978 et n° 2018-493 du 20 juin 2018 dites «Informatique et Libertés» et le règlement général (UE) 2016/679 du 27 avril 2016 relatif à la protection des données (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.

Ces données sont placées sous la responsabilité de l'ECL, agissant en qualité de responsable de traitement, conformément au principe dit de l'accountability (article 24 du Règlement Général sur la Protection des Données).

Chaque utilisateur dispose d'un droit d'accès, de rectification et d'opposition à l'égard des données le concernant, y compris les données portant sur l'utilisation des systèmes d'Information.

Ce droit s'exerce auprès du Délégué à la Protection des Données. (dpd.rgpd@listes.ec-lyon.fr)

ARTICLE VIII. LIMITATIONS DES USAGES

En cas de non-respect des règles définies dans la présente charte et des modalités définies dans les guides d'utilisation, le directeur ou les responsables sécurité du système d'information pourront, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des personnels, limiter les usages par mesure conservatoire.

Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extra-professionnelles, est passible de sanctions.
Elles sont décidées par la section disciplinaire de L'ECL prévue à l'article L 712-4 du code de l'éducation. Les sanctions encourues sont fixées par l'article R-811 du code de l'éducation.

ARTICLE IX. ENTREE EN VIGUEUR DE LA CHARTE

La présente charte est adossée au règlement intérieur et en constitue un élément indissociable. Son approbation se fait dans les mêmes conditions de forme que le règlement intérieur de l'établissement.

Le présent document annule et remplace tous les autres documents ou chartes relatifs à l'utilisation des systèmes d'Information.

RAPPELS JURIDIQUES
Cette liste non exhaustive est produite à titre d'information

L'école et l'utilisateur sont tenus de respecter les dispositions légales et règlementaires suivantes :

- Circulaire PM N°5725, signée le 17 juillet 2014, portant sur la mise en œuvre de la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE)
- Décret n° 2011-1425 du 2 novembre 2011 portant application de 1' article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation.
- Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation.
- Circulaire interministérielle de la mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation du 7 novembre 2012.

L'utilisation des ressources informatiques dans l'école n'a pas lieu en dehors du droit.

- le respect des personnes (pas d'atteinte à la vie privée ou au secret de la correspondance, ni d'injures ou de diffamation) et respect des systèmes d'informations (Crimes et délits contre les biens); *Article 9 du Code civil, Articles : 226-1,226-15, 222-17, R 621-2, 226-10 du Code pénal, art.432-9 modifié par la loi nº2004-669 du 9 juillet 2004, Article 29 de la Loi du 29 juillet 1881, Article 26, 27,34, 36 de la Loi n° 78-17 du 6 janvier 1978, art. 313-1 et suite 323-1 à 323-7 modifiés par la loi nº 2004-575 du 21 juin 2004 du Code pénal*
- la protection des mineurs contre les contenus dégradants, violents ou favorisant sa corruption ; *Article 227-24, 227-23 du Code pénal, Loi 2004- 575 du 21 juin 2004*
- le respect de l'ordre public qui condamne le racisme, l'antisémitisme ou l'apologie du crime ; *Article 24 et 24bis de la Loi du 29 juillet 1881, Article L 323-1 et s. du Code pénal*
- le respect du droit d'auteur des œuvres littéraires, musicales, photographiques ou audiovisuelles mises en ligne, respect de la propriété intellectuelle pour les logiciels. *Article L 335-3, L 111-1, L 121-1, L 122-1, L 123-2, L 131-2 du Code de propriété intellectuelle*
- Protection contre les délits informatiques : pénétration non autorisée sur un système automatisé, destruction ou modification de données, introduction frauduleuse de données, entrave au fonctionnement ; *loi du 5 janvier 1988 dite « loi Jacques Godfrain » et ses 7 articles (323-1 à 323-7).*
- Loi de conservation des données de connexion :
  « les opérateurs de communications électroniques conservent pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales : les informations permettant d'identifier l'utilisateur, les données relatives aux équipements terminaux de communication utilisés, les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication, les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs, les données permettant d'identifier le ou les destinataires de la communication. »
  Décret n°2006-358 du 24 mars 2006 Art. R. 10-13.- I