RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

UNIVERSITÉ CÔTE D'AZUR

CHARTE DE BON USAGE DES RESSOURCES INFORMATIQUES

La présente charte a pour objet de définir les règles d'utilisation des moyens et systèmes informatiques d'Université Côte d'Azur. La charte est annexée au règlement intérieur de l'établissement. Elle pourra évoluer en fonction du contexte légal et de la politique de sécurité notamment applicable au sein de l'établissement

1. Champ d'application de la charte

Les règles et obligations ci-après s'appliquent à toute personne autorisée à utiliser les moyens et systèmes informatiques d'Université Côte d'Azur. Sont concernés les étudiantes et les étudiants, les enseignantes et les enseignantes, les chercheuses et les chercheurs, les biatss et les personnels invités. Les moyens et systèmes informatiques de l'établissement incluent notamment les serveurs, stations de travail et micro-ordinateurs des services, des salles de cours ou de travaux pratiques et des laboratoires qu'ils soient ou non connectés au réseau, les routeurs, commutateurs, points d'accès Wi-Fi, câbles et fibres optiques. Ces règles s'étendent également à l'utilisation des systèmes informatiques extérieurs à l'Université accessibles via les réseaux de l'établissement et notamment Internet.

2. Conditions d'accès aux réseaux informatiques d'Université Côte d'Azur

Le droit d'accès à une ressource informatique est :

- Soumis à autorisation et assorti de moyens d'identification : il peut être retiré si les conditions d'accès ne sont plus respectées ou si le comportement de l'utilisatrice ou de l'utilisateur est contraire à la charte ;

- Personnel et incessible : chaque utilisatrice et utilisateur se voit attribuer un identifiant informatique. Le mot de passe choisi doit être difficilement devinable, strictement confidentiel et ne doit sous aucun prétexte être communiqué à une tierce personne. Il doit être modifié à minima une fois par an. Les moyens d'accès et d'identification auxquels donne droit l'appartenance à Université Côte d'Azur tels que : adresse électronique, clé, carte magnétique, code, mot de passe, sont personnels et ne doivent en aucun cas être cédés.

- Il est limité à des activités reconnues par l'Université. L'utilisation des ressources informatiques de l'établissement a pour objet exclusif de mener des activités de recherche, d'enseignement, d'administration ou d'insertion professionnelle. Sauf autorisation préalable dûment délivrée par l'établissement, ces moyens ne peuvent être utilisés pour réaliser des projets ne relevant pas des missions confiées aux utilisatrices et utilisateurs.

3. Règles d'utilisation des ressources informatiques

Les utilisatrices et utilisateurs sont responsables, en tout lieu, de l'usage qu'ils font du système d'information d'Université Côte d'Azur. Ils sont tenus à une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels elles et ils accèdent.

- Chaque utilisatrice et utilisateur se doit d'utiliser les logiciels dans les conditions des licences souscrites et de ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies, sons, vidéos ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits ;
- Chaque utilisatrice et utilisateur s'engage à ne pas de tenter d'installer des logiciels ou applications pour lesquels l'établissement ne possèderait pas un droit d'usage ;
- Toute communication de nature professionnelle, à diffusion interne ou externe, devra être effectuée au moyen de l'adresse institutionnelle de l'établissement ou de l'un de ses partenaires ;
- Toute information est réputée professionnelle à l'exclusion des données désignées comme relevant de sa vie privée : dans ce cas, il appartient à l'utilisatrice ou à l'utilisateur de procéder au stockage de ces données à caractère privé dans des répertoires explicitement prévus à cet effet et clairement identifiés comme privés. La protection et la sauvegarde de ces données sont de sa responsabilité. L'établissement ne peut être engagé à conserver cet espace ;
- Chaque utilisatrice et chaque utilisateur est responsable de son adresse électronique nominative délivrée par Université Côte d'Azur. Tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé. Sont interdits les messages comportant des contenus à caractère illicite quelle qu'en soit la nature ;
- Chaque utilisatrice et chaque utilisateur doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages, et 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 ;
- Les communications syndicales, quel qu'en soit le canal de diffusion, doivent respecter les dispositions législatives et réglementaires en vigueur, en particulier celles du décret n° 82-2/4447 du 28 mai 1982 relatif à l'exercice du droit syndical dans la fonction publique modifié.

Dans le cadre du respect des règles de déontologie informatique, les utilisatrices et utilisateurs s'engagent notamment à ne pas :

- Nuire à l'activité professionnelle d'un tiers par l'utilisation des moyens informatiques,
- Usurper l'identité d'une autre personne,
- Intercepter les communications entre tiers,
- S'approprier le mot de passe d'un autre utilisateur,
- Altérer des données ou accéder à des informations appartenant à d'autres utilisateurs du réseau sans autorisation,
- Se connecter sur un serveur d'Université Côte d'Azur sans y être autorisé,
- Dissimuler sa véritable identité,
- Connecter directement aux réseaux physiques des matériels autres que ceux confiés ou autorisés par l'établissement

- Développer, installer ou copier un programme pour contourner la sécurité ou saturer les ressources informatiques,
- Introduire volontairement des logiciels parasites (virus, chevaux de Troie,...),

4. Protection des données à caractère personnel

4.1 Devoirs des utilisateurs

- Les utilisatrices et utilisateurs sont informés de la nécessité de respecter les dispositions légales en matière de traitements automatisés ou manuels de données à caractère personnel, prévues pour l'essentiel dans la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi « Informatique et libertés » en vigueur et le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018.
- Dans ce cadre, les utilisatrices et utilisateurs devront informer le Délégué à la protection des données (dpo@univ-cotedazur.fr) et se conformer à la procédure en vigueur pour la mise en œuvre d'un traitement de données à caractère personnel.
- Conformément à la législation applicable à la protection des données personnelles, les principes directeurs à respecter dans le cadre de la mise en œuvre d'un traitement de données personnelles sont les suivants :
    - Le respect des finalités initiales du traitement ;
    - La pertinence et l'exactitude des données au regard des finalités poursuivies ;
    - L'information des personnes à la collecte des données et la conservation du recueil de leur consentement en cas de signature électronique ou manuscrite ;
    - Le droit d'accès, de rectification ;
    - Le droit d'opposition ;
    - La mise en œuvre de mesures de sécurité adaptées à la sensibilité des données traitées, résultant d'une étude d'impact pour les personnes privées en cas de divulgation, altération ou destruction des données les concernant.
    - Le contrôle rigoureux de la diffusion de données à caractère personnel à l'attention de tiers extérieurs, en incluant notamment les clauses adaptées dans les contrats avec les sous-traitants.
    - La destruction des données au-delà de la période de conservation prévue.

4.2 Droits des utilisateurs

- L'établissement met en œuvre des traitements de données à caractère personnel en relation avec l'usage et la sécurité des systèmes d'information et de communication couverts par la présente charte. L'établissement s'engage à ce que les données concernant les utilisatrices et utilisateurs soient collectées et traitées de manière loyale et licite, dans les conditions exposées.
    - Université Côte d'Azur a désigné un Délégué à la Protection des Données joignable à l'adresse dpo@univ-cotedazur.fr
- Les catégories suivantes de données sont traitées :
    - Informations professionnelles
    - Informations relatives à l'identité (y.c. photo d'identité)
    - Coordonnées professionnelles
    - Informations sur l'utilisation des systèmes d'information et de communication.

- Ces catégories de données proviennent essentiellement des systèmes d'information et de communication ainsi que des annuaires informatiques et des directions des ressources humaines.
- Ces données sont conservées selon les durées légales.
- Ces données sont destinées à l'établissement ainsi qu'aux personnes habilitées au sein de l'établissement et aux autorités habilitées.
- Les traitements opérés dans le cadre de la charte ont pour finalité :
    - Le suivi et la maintenance des systèmes d'information et de communication, qu'il s'agisse des applications informatiques internes ou des accès vers l'extérieur (soit notamment l'accès à internet) ;
    - La gestion des annuaires et référentiels permettant de définir les autorisations d'accès aux applications et réseaux ;
    - La mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement des systèmes d'information et de communication, notamment la conservation des journaux de connexion, des traces informatiques et des données de toute nature ;
    - La gestion de la messagerie électronique ;
    - Le contrôle du respect de la charte et les audits de sécurité ;
- Conformément à la loi « Informatique et libertés », les utilisatrices et utilisateurs sont informés, en particulier, qu'ils disposent d'un droit d'interrogation, d'accès, de limitation, d'effacement, de rectification et d'opposition au traitement des données les concernant et qui s'exerce auprès du Délégué à la protection des données (dpo@univ-cotedazur.fr). Par ailleurs, ils disposent d'un droit de réclamation auprès de la Cnil.

5. Mise à disposition d'équipements informatiques et numériques et restitution

Les matériels et terminaux mis à la disposition de l'utilisateur par l'Université (sont inclus tout matériel financé par des contrats ou conventions obtenus au titre de l'établissement) restent la propriété de l'Université. Les utilisatrices et utilisateurs s'engagent à utiliser ce matériel dans les règles prévues à cet effet et à signaler immédiatement tout problème constaté (panne, casse, perte ou vol) à l'Université. Toute dégradation volontaire du matériel est imputable à son auteur : la réparation est assurée aux frais des auteurs de la dégradation, sans présumer des sanctions disciplinaires qui pourraient être prises. Par ailleurs, l'établissement représenté par son président est fondé à faire valoir ses droits à réparations, et obtenir le dédommagement des préjudices subis.

Les utilisatrices et utilisateurs s'engagent à restituer tous les équipement perçus (ordinateur, téléphones, accessoires et périphériques …) à la fin de son contrat. Le défaut de restitution par le salarié du matériel confié (ex : téléphone, ordinateur, tablette, etc.) constitue un délit d'abus de confiance puni par l'article 314-1 du Code pénal.

6. Sécurité et vigilance

Université Côte d'Azur veille à la bonne utilisation des ressources matérielles et logicielles ainsi que des échanges électroniques. Elle se réserve le droit de limiter le téléchargement de certains fichiers trop volumineux ou présentant un risque pour la sécurité des systèmes (virus susceptibles d'altérer le bon fonctionnement du système d'information de l'institution, codes malveillants, programmes espions ...).

Chaque utilisatrice et utilisateur a la charge, à son niveau, de contribuer à la sécurité des systèmes d'information et de communication mis à sa disposition. Il convient de veiller tout particulièrement à ne pas transporter d'informations sensibles sans protection sur des supports non fiabilisés (clés USB, ordinateurs portables, disques externes...) et à ne pas quitter leur poste de travail ni ceux en libre-service en laissant des ressources ou services accessibles. Les recommandations sur la sécurité de l'établissement et la protection des données sensibles doivent être suivies.

Ils devront donc veiller à :

- Prévenir immédiatement les équipes informatiques de tout accès frauduleux ou tentative d'accès aux ressources qu'ils utilisent ;
- Prendre toute disposition utile pour permettre l'accès à ses données professionnelles aux personnes habilitées, aux seules fins d'assurer la continuité de service en cas d'absence ou de départ. Les dispositions nécessaires pour garantir la conservation de ces informations seront prises, de son côté, par le responsable hiérarchique.
- Se conformer notamment, mais non limitativement, aux règles de conduite suivante :
    - Ne pas ouvrir les pièces jointes reçues de l'extérieur quand l'émetteur du message est inconnu ou douteux ;
    - Ne pas modifier ou détruire, ou tenter de modifier ou détruire, des fichiers sur lesquels il ne dispose d'aucun droit ;
    - Ne pas mettre à la disposition de personnes non autorisés un accès aux systèmes d'information et de communication ou aux réseaux à travers les matériels utilisés ;
    - Ne pas utiliser ou tenter d'utiliser des comptes autres que ceux qui lui sont attribués ou masquer son identité ;
- En cas de réception de messages non sollicités (spams), et notamment en cas de tentative de phishing visant à obtenir ses identifiants :
    - Ne pas l'ouvrir sans s'être assuré préalablement de son innocuité ;
    - Ne pas y répondre ;
    - En cas de doute, transférer le message reçu à abuse@univ-cotedazur.fr ou contacter par formulaire l'assistance informatique.
- Signaler, sans délai, tout dysfonctionnement, altération, perte, vol, destruction et autre événement pouvant affecter les systèmes d'information et de communication.

7. Contrôles, opération de maintenance et suivi des consommations

7.1 Contrôles pouvant être opérés

- L'établissement est soumis à une obligation générale de sécurité, en application des dispositions du Code pénal relatives à la protection des systèmes de traitement automatisés de données, et de la loi dite « Informatique et Libertés ».
- Les infrastructures informatiques d'Université Côte d'Azur peuvent 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.
- L'établissement, en tant qu'employeur, dispose également d'un pouvoir de contrôler l'activité des utilisateurs et en particulier, le respect par eux de la charte.
- L'utilisation des moyens et ressources informatiques et numériques pourra faire l'objet d'une surveillance afin de détecter toute utilisation non conforme, d'optimiser cette même utilisation ou encore de mener des analyses statistiques.

- L'établissement se réserve ainsi le droit, notamment :
  - De vérifier le trafic informatique entrant et sortant, ainsi que le trafic transitant sur le réseau interne ;
  - De diligenter des audits pour vérifier que les consignes d'usage et les règles de sécurité et de sûreté sont appliquées sur les ressources du système d'information ;
  - De contrôler l'origine licite des logiciels installés ;
  - De conserver des fichiers de journalisation des traces en fonction des besoins propres de chaque système d'information ;
  - De transmettre aux autorités judiciaires sur requête tout ou partie des enregistrements disponibles.
- En outre, en cas d'incident, l'établissement se réserve le droit de :
  - Surveiller le contenu des informations qui transitent sur son système d'information ;
  - Vérifier le contenu des disques durs des ressources du système d'information attribuées aux utilisatrices et utilisateurs ;
  - Procéder à toutes copies utiles pour faire valoir ses droits.

Les agents/personnels de ce service disposent d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place. Ils ont accès à l'ensemble des données techniques enregistrées mais s'engagent à respecter les règles de confidentialité applicables aux contenus des documents. Ils sont assujettis au devoir de réserve et sont tenus de préserver la confidentialité des données qu'ils sont amenés à connaître dans le cadre de leurs fonctions.

7.2 Maintenance

- La mise à disposition de moyens et ressources informatiques et numériques implique nécessairement des opérations de maintenance technique (maintenance corrective, maintenance préventive ou évolutive), et ce, pour assurer le bon fonctionnement et la sécurité de ceux-ci.
- Ces opérations prennent la forme d'une intervention d'une « personne habilitée » soit sur site, soit à distance, conduisant alors cette personne à effectuer une « prise en main à distance » selon un calendrier préétabli ou en cas d'incident.
- En aucun cas, ces opérations, quel que soit leur mode opératoire, ne justifient le fait pour l'utilisateur de communiquer ses moyens d'authentification.
- Dans ce cadre, la « personne habilitée » peut être amenée à avoir accès à l'ensemble des éléments présent sur le poste ou le matériel nomade de l'utilisatrice et l'utilisateur, ainsi que des données de connexion, qu'il s'agisse d'un usage professionnel ou privé.

7.3 Suivi des consommations

- Pour la bonne gestion des ressources liées aux systèmes d'information et de communication :
  - Pour la téléphonie fixe, les éléments de la communication (date, heure, durée, coût et numéros appelés) le contrôle des consommations peut être effectué sur la base des factures détaillées sans divulgation des 4 derniers digits des numéros appelés ;

- Pour les systèmes d'information et de communication nomades, les éléments de la communication (date, heure, durée, coût et numéros appelés) sont disponibles via les opérateurs téléphoniques mobiles, à travers les services de suivi des consommations qu'ils proposent.

- L'enregistrement des conversations téléphoniques est strictement interdit, sauf à en informer préalablement l'interlocuteur.

8. Responsabilité et sanctions

- L'utilisateur est responsable :
  - Dans le cadre de son activité professionnelle, de l'utilisation des moyens et ressources informatiques et numériques en conformité avec la présente charte ;
  - Dans la sphère de sa vie privée résiduelle, seul, à l'exclusion donc de toute responsabilité de l'établissement, de tout usage des moyens et ressources informatiques et numériques à caractère non professionnel. En effet, si une utilisation résiduelle privée peut être tolérée, les connexions établies grâce à l'outil informatique ou aux réseaux mis à disposition par l'administration sont présumées avoir un caractère professionnel.
- Le non-respect des règles édictées par la présente charte pourra donner lieu, indépendamment à d'éventuelles sanctions civiles et/ou pénales, à la suspension temporaire ou définitive de l'accès aux ressources informatiques de l'Université ainsi qu'à des sanctions disciplinaires internes

Le présent document annule et remplace tout autre document ou charte afférent à l'utilisation des ressources informatiques d'Université Côte d'Azur.