

CHARTRE POUR L'USAGE DU SYSTÈME D'INFORMATION ET DES SERVICES NUMÉRIQUES

1. Objet et champ d'application

La présente charte définit les droits et obligations des utilisateurs de l'ensemble des moyens informatiques matériels et logiciels, des réseaux et des outils de communication numérique mis à leur disposition par l'Université d'Avignon et des Pays de Vaucluse (UAPV).

L'accès distant à cet ensemble, par un poste fixe ou nomade (tablette, smartphone, ordinateur portable, etc.) relève également de cette charte.

Les utilisateurs sont ceux auxquels l'UAPV a attribué un compte :

- les usagers de l'UAPV,
- les personnels de l'UAPV,
- les personnes invitées par l'UAPV et utilisatrices d'un compte provisoire.

La présente charte a été adoptée par le Conseil d'Administration de l'UAPV le 26 septembre 2017. Elle est annexée au règlement intérieur général de l'UAPV et portée à la connaissance des utilisateurs.

L'utilisation de l'ensemble des moyens informatiques matériels et logiciels, des réseaux et des outils de communication numérique de l'UAPV est subordonnée à l'acceptation sans réserve de cette charte.

2. Conditions d'accès

Chaque utilisateur se voit attribuer un compte, déterminé par un identifiant et un mot de passe, qu'il lui appartient de modifier ultérieurement, lui permettant de se connecter aux services numériques. Ces identifiant et mot de passe sont strictement personnels et ne peuvent en aucun cas être cédés ou communiqués, même temporairement, à un tiers, y compris aux personnels informaticiens de l'UAPV qui n'en font jamais la demande.

Le non-respect des règles définies dans la présente charte entraîne automatiquement la fin de l'autorisation de connexion aux services numériques.

3. Règles générales d'usage

De manière générale, l'utilisation des services numériques doit respecter les dispositions légales et réglementaires. Elle doit être rationnelle et loyale afin d'en éviter la saturation ou le détournement à des fins personnelles.

3.1 Finalité, usage professionnel / privé

Les services numériques sont mis à disposition des utilisateurs pour un usage universitaire relevant des missions de l'UAPV, c'est-à-dire un usage professionnel pour les personnels et strictement lié à leurs études pour les usagers.

Cependant, une utilisation résiduelle à titre privé est autorisée sous réserve d'être non lucrative, raisonnable dans la fréquence et la durée, et de ne pas nuire à la qualité et au fonctionnement du service.

Toute information stockée sur les ressources de l'UAPV 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 prévu explicitement à cet effet, par exemple un répertoire ou dossier intitulé « privé ». La protection et la sauvegarde des données à caractère privé incombent à l'utilisateur. L'UAPV ne peut être tenue pour responsable de la perte de ces données.

3.2 Respect de la propriété intellectuelle

L'utilisateur doit respecter les dispositions légales et réglementaires concernant la propriété intellectuelle.

Il doit notamment ne pas copier, diffuser, modifier ou utiliser les logiciels, base de données, pages web, textes, images, sons ou autres créations protégées par le droit d'auteur sans avoir obtenu l'autorisation des titulaires de ces droits.

3.3 Respect des dispositions de la loi Informatique et Libertés

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés a créé un dispositif juridique pour encadrer la mise en œuvre des traitements automatisés de données à caractère personnel.

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

L'utilisateur doit, avant toute création de fichier comprenant ce type d'informations, y compris lorsqu'elle résulte d'interconnexion de fichiers existants, saisir le Correspondant Informatique et Libertés de l'UAPV (CIL ou Data Protection Officer, cil@univ-avignon.fr).

A l'UAPV, le droit d'accès et de rectification sur les données à caractère personnel s'exerce auprès du Correspondant Informatique et Liberté dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

3.4 Sécurité

La protection des Systèmes d'Information (SI) s'appuie sur des dispositions légales qui prévoient que sont interdits :

- l'accès illicite, c'est-à-dire toute introduction dans un SI par une personne non autorisée ;
- le maintien frauduleux ou irrégulier dans le SI (le fait de s'y maintenir i.e. de le parcourir même sans altération de données alors que les éléments accessibles sont perçus comme ne devant pas l'être) ;
- l'entrave au système, c'est à dire toute perturbation volontaire du fonctionnement d'un SI ;
- 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 ;
- le fait, sans motif légitime, d'importer, de détenir ou de mettre à disposition un équipement, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions décrites ci-dessus.

L'utilisateur :

- doit choisir un mot de passe sûr et le garder strictement confidentiel ; si, pour quelque raison que ce soit, l'utilisateur est informé ou estime que ses codes d'accès ne sont plus confidentiels, il doit procéder dès que possible au changement de ces derniers ;
- ne doit pas utiliser les codes d'accès d'un autre utilisateur, ni chercher à les connaître ;
- ne doit pas tenter de masquer son identité, ni d'usurper l'identité d'un tiers ;
- ne doit pas tenter d'accéder aux données d'autrui, même si elles ne sont pas protégées, ni aux communications entre tiers ;
- ne doit pas tenter d'accéder à des ressources pour lesquelles il n'a pas reçu d'habilitation ;
- ne doit pas utiliser les services qui lui sont offerts pour proposer ou rendre accessibles à des tiers des informations confidentielles ou des données dont le contenu serait contraire à la législation ;
- ne doit pas apporter de perturbations au bon fonctionnement du SI et du réseau par des manipulations anormales de matériel ou par l'introduction de logiciels parasites ;
- ne doit pas quitter son poste de travail ou un poste en libre-service en laissant des ressources ou services accessibles ;
- doit informer le Responsable de la Sécurité des Systèmes d'Information (RSSI) de l'UAPV (rssi@univ-avignon.fr) de toute anomalie constatée (intrusion, altération, destruction, possibilité anormale d'accès à une ressource, etc.).

L'utilisation d'outils externes conduisant à faire transiter ou à déposer des informations professionnelles et/ou pédagogiques hors des supports et technologies mis en œuvre par l'UAPV présente un risque de vulnérabilité particulier du point de vue de la confidentialité des données, de la protection du patrimoine scientifique, technique, littéraire, etc. mais également des libertés individuelles.

En particulier, l'utilisateur ne doit pas transporter sans protection (telle qu'un chiffrement) des données sensibles sur des supports tels qu'ordinateurs portables, clés USB, disques externes, etc. ni utiliser de services externes pour les échanges ou le dépôt de telles données. Ces pratiques engagent la responsabilité de l'utilisateur.

4. Usage des moyens de communication numérique

Les moyens de communication numérique recouvrent le web, la messagerie (y compris les listes de diffusion), la messagerie instantanée, les forums, la téléphonie par Internet, la visioconférence, les espaces de travail collaboratif et toute forme d'accès aux réseaux.

Conformément aux dispositions du code pénal, l'utilisateur ne doit pas diffuser d'informations ou données dont le contenu présente un caractère illégal, notamment raciste, diffamatoire ou injurieux. L'utilisateur doit respecter les règles de politesse d'usage. La responsabilité de l'utilisateur pourra être engagée en cas de non-respect des dispositions législatives, réglementaires et statutaires en vigueur.

Le fait d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises ou reçues par la voie de communications numériques peut également faire l'objet de sanctions pénales (art. 226-15 du code pénal).

Les courriers électroniques à caractère professionnel pour les personnels de l'UAPV, ou liés à leurs études pour les usagers, doivent être adressés au moyen de l'adresse électronique fournie par l'UAPV.

5. Maintenance, surveillance, traces et contrôles

Les opérations nécessaires de maintenance technique (corrective, évolutive ou préventive) sur les services numériques sont réalisées avec un souci de moindre perturbation du service et sont, dans la mesure du possible, annoncées à l'avance.

L'utilisateur dont le poste de travail fait l'objet d'une maintenance à distance est préalablement informé.

Un système de journalisation de l'utilisation des services numériques ainsi que des outils de traçabilité sont mis en œuvre par l'UAPV, conformément à la législation en vigueur.

Pour des nécessités de gestion technique, de contrôle à des fins statistiques, d'optimisation, de sécurité ou de détection des abus, l'utilisation des services numériques peut être analysée et contrôlée. Ces opérations sont menées exclusivement par les personnels habilités, dans le respect de la législation applicable et notamment de la loi relative à l'informatique et aux libertés. Ces derniers sont soumis à une obligation de confidentialité. Ils ne peuvent donc divulguer les informations qu'ils sont amenés à connaître dans le cadre de leur fonction, sous réserve de la loi (art. 40, al. 2, du code de procédure pénale) qui dispose que « *Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs* ».

En outre, ces personnels habilités peuvent être amenés à prendre des mesures conservatoires pour faire cesser rapidement tout abus constaté.

6. Modification de la Charte

Dans le respect des compétences des instances de l'UAPV et des procédures réglementaires, la présente charte pourra être modifiée sans préavis. Ces éventuelles modifications entreront en vigueur dès leur publication.

Je soussigné(e)

Reconnais avoir pris connaissance de cette charte

Le/...../..... Signature