Charte d'usage du système d’information

Institut polytechnique de Grenoble,
Institut d'ingénierie et de management,
Université Grenoble Alpes

Sommaire

Préambule 3

Article I. Champ d'application 4

Article II. Droit d'accès aux systèmes d'information 4

Article III. Protection des données 4

Article IV. Conditions d'utilisation des systèmes d'information 4

Section IV.1 Utilisation professionnelle / privée 4

Section IV.2 Continuité de service : gestion des absences et des départs 5

Article V. Principes de sécurité 5

Section V.1 Règles de sécurité applicables 5

Section V.2 Devoirs de signalement et d'information 6

Section V.3 Mesures de contrôle 6

Article VI. Communication électronique 7

Section VI.1 Messagerie électronique 7

(a) Adresses électroniques 7

(b) Contenu des messages électroniques 7

(c) Émission et réception des messages 7

(d) Statut et valeur juridique des messages 7

(e) Stockage et archivage des messages 8

Section VI.2 Internet 8

(a) Publication sur les sites Internet et Intranet de l'établissement 8

(b) Sécurité 8

Section VI.3 Téléchargements 8

Article VII. Traçabilité 8

Article VIII. Respect de la propriété intellectuelle 9

Article IX. Respect de la législation sur les données personnelles 9

Article X. Limitation des usages 9

Article XI. Entrée en vigueur de la charte 9

Annexe 10

Principales références légales 10

(a) Infractions prévues par le Nouveau Code pénal 10

(b) Infractions de presse (loi 29 juillet 1881, modifiée) 10

(c) Infraction au Code de la propriété intellectuelle 10

Préambule

Le « système d'information » recouvre l'ensemble des données et des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunication locaux, ainsi que ceux auxquels il est possible d'accéder à distance ou en cascade à partir des réseaux de l'Institut polytechnique de Grenoble, Institut d'ingénierie et de management, Université Grenoble Alpes.

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

Le terme d'« utilisateur » recouvre toute personne ayant vocation à détenir un compte informatique ou à avoir accès aux ressources du système d'information quel que soit son statut.

Il s'agit notamment de :

- *tout agent titulaire ou non titulaire concourant à l'exécution des missions du service public de l'enseignement et de la recherche ;*
- *tout étudiant inscrit dans l'établissement ;*
- *toute personne extérieure à l'établissement, visiteur, invité, prestataire*[1] *ayant contracté avec l'établissement.*

Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires, notamment le respect des règles visant à assurer la sécurité, la performance des traitements et la conservation des données.

La présente charte définit les règles d'usage et de sécurité que l'établissement et l'utilisateur s'engagent à respecter : elle précise les droits et les devoirs de chacun.

Engagements de l'établissement

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

L'établissement met en œuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisateurs.

L'établissement facilite l'accès des utilisateurs aux ressources du système d'information. Les ressources mises à leur disposition sont prioritairement à usage professionnel mais l'établissement est tenu de respecter l'utilisation résiduelle du système d'information à titre privé.

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 qu'il produit ou auxquels il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie[2].

En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat.

L'utilisation des ressources qui sont mises à sa disposition doit être rationnelle et loyale afin d'en éviter la saturation ou le détournement à des fins personnelles.

1 Le contrat devra prévoir expressément l'obligation de respect de la charte.
2 Notamment le secret médical dans le domaine de la santé.

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 de ses utilisateurs.

Les usages relevant spécifiquement de l'activité des organisations syndicales ne sont pas régis par la présente charte.

Ces règles s'appliquent à toute personne autorisée à utiliser les moyens informatiques de l'établissement, y compris les moyens informatiques mutualisés ou externalisés, et s'étendent aux réseaux extérieurs accessibles par l'intermédiaire des réseaux de l'établissement.

Article II. Droit d'accès aux systèmes d'information

Le droit d'accès aux systèmes d'information est temporaire. Il est retiré si la qualité de l'utilisateur ne le justifie plus et, sauf demande expresse, au plus tard 3 mois après que celui-ci n'ait plus vocation à détenir un compte informatique.

Il peut également être retiré, par mesure conservatoire, si le comportement de l'utilisateur n'est plus compatible avec les règles énoncées dans la présente charte.

Article III. Protection des données

L'utilisateur est responsable de ses données professionnelles, ou de celles auxquelles il a accès dans le cadre de ses fonctions. Il doit en particulier s'assurer de la sauvegarde de ses données, et être vigilant sur les droits d'accès qu'il donne aux autres utilisateurs sur celles-ci.

L'utilisateur doit assurer la protection des informations sensibles (pour lesquelles a été identifié un besoin direct ou indirect de confidentialité) ; il doit notamment éviter de les communiquer ou les transporter sans protection (chiffrement) via des supports non fiabilisés (messagerie, clés USB, ordinateurs portables, disques externes, etc.) et ne pas les déposer sur un serveur externe ou ouvert au grand public.

Les mesures de conservation des données professionnelles sont définies avec le responsable désigné au sein de l'établissement.

Article IV. Conditions d'utilisation des systèmes d'information

Section IV.1 Utilisation professionnelle / privée

L'utilisation des systèmes d'information de l'établissement a pour objet exclusif de mener des activités de recherche, d'enseignement, de documentation, d'administration ou de vie universitaire. Sauf autorisation, ces moyens ne peuvent être employés en vue d'une utilisation ou de la réalisation de projets ne relevant pas des missions de l'établissement ou des missions confiées aux utilisateurs. Ils peuvent néanmoins constituer le support d'une communication privée dans les conditions décrites ci-dessous.

L'utilisation résiduelle du système d'information à titre privé doit être non lucrative et raisonnable, tant dans sa fréquence que dans son volume ou dans sa durée. En toute hypothèse, le surcoût qui en résulte doit demeurer négligeable au regard du coût global d'exploitation.

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 réputée professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée, quel que soit le support (ordinateur, clé USB, téléphone…) ou le service (espace de stockage, messagerie…) utilisés.

Ainsi, il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu explicitement[3] à cet effet ou en mentionnant le caractère privé sur la

3 Pour exemple, cet espace pourrait être dénommé "_privé_"

ressource[4]. La protection et la sauvegarde régulière des données à caractère privé incombent à l'utilisateur.

L'utilisateur est responsable de son espace de données à caractère privé. Lors de son départ définitif de l'établissement, il lui appartient de détruire son espace de données à caractère privé, la responsabilité de l'établissement ne pouvant être engagée quant à la conservation de cet espace. En cas de décès de l'utilisateur, ses espaces privés seront effacés.

L'utilisation des systèmes d'information à titre privé doit respecter la réglementation en vigueur.

En particulier, la détention, diffusion et exportation d'images à caractère pédophile[5], ou la diffusion de contenus à caractère raciste ou antisémite[6] est totalement interdite.

Par ailleurs, eu égard à la mission de l'établissement, la consultation de sites de contenus à caractère pornographique depuis les locaux de l'établissement, hors contexte professionnel, est interdite.

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

Afin d'assurer la continuité de service, l'utilisateur doit privilégier le dépôt de ses fichiers de travail sur des zones partagées par les membres de son service ou de son équipe. En tout état de cause les données non situées dans un espace identifié comme privé, sont considérées comme appartenant à l'établissement qui pourra y accéder librement.

En cas de départ, ou d'absence prolongée, l'utilisateur informe sa hiérarchie des modalités permettant l'accès aux ressources mises spécifiquement à sa disposition. Ces modalités respectent les règles de sécurité énoncées à la Section V.1

Article V. Principes de sécurité

Section V.1 Règles de sécurité applicables

L'établissement met en œuvre les mécanismes de protection appropriés sur les systèmes d'information 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. 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, notamment les règles relatives à la gestion des codes d'accès ; chaque utilisateur est responsable de l'utilisation qui en est faite.
- de garder strictement confidentiels son (ou ses) codes d'accès et ne pas le(s) dévoiler à un tiers ;
- de respecter la gestion des accès, en particulier ne pas utiliser les codes d'accès d'un autre utilisateur, ni chercher à les connaître.
- de veiller à ne pas laisser leur poste de travail en libre accès.

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

✓ de la part de l'établissement :

- 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 ;

4 Pour exemple, "_privé_nom_de_l_objet_" : l'objet pouvant être un message, un fichier ou toute autre ressource numérique.
5 Article L 323-1 et s. du Code pénal
6 Article 24 et 26bis de la Loi du 29 juillet 1881

- ✓ 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 par l'établissement, ou ceux dont la liste a été précisée dans un guide d'utilisation établi par le service ou l'établissement ;
- ne pas installer, télécharger ou utiliser sur le matériel de l'établissement, des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, ou sans autorisation de l'établissement ;
- se conformer aux dispositifs mis en place par l'établissement pour lutter contre les virus et les attaques par programmes informatiques ;
- s'engager à ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations anormales du matériel ou du logiciel ;
- veiller à protéger les matériels mis à sa disposition contre le vol et les dégradations ;
- appliquer les recommandations sécurité de l'établissement.

Section V.2 Devoirs de signalement et d'information

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

Section V.3 Mesures de contrôle

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 pour le système ou générant une difficulté technique d'acheminement à son destinataire, sera isolée ; le cas échéant supprimée.
- 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.

Les personnels chargés des opérations de contrôle des systèmes 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 qu'identifiées comme telles, elles relèvent de la vie privée de l'utilisateur.
- elles ne mettent pas en cause le bon fonctionnement technique des applications ou leur sécurité,
- elles ne tombent pas dans le champ de l'article[7] 40 alinéa 2 du code de procédure pénale.

7 Obligation faite à tout fonctionnaire d'informer sans délai le procureur de la République de tout crime et délit dont il a connaissance dans l'exercice de ses fonctions.

Article VI. Communication électronique

Section VI.1 Messagerie électronique

L'utilisation de la messagerie constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'échange 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 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.

Une adresse électronique, fonctionnelle ou organisationnelle, peut être mise en place pour un utilisateur ou un groupe d'utilisateurs pour les besoins de l'établissement.

La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles, désignant une catégorie ou un groupe d'« utilisateurs », relève de la responsabilité exclusive de l'établissement : ces listes ne peuvent être utilisées sans autorisation

(b) Contenu des messages électroniques

Tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé[8] ou s'il est stocké dans un espace privé de données.

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place. En particulier des solutions de traitement des messages indésirables (spam, contrôle des virus…) pourront être déployées.

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 (par exemple : atteinte à la tranquillité par les menaces, atteinte à l'honneur par la diffamation, atteinte à l'honneur par l'injure non publique, protection du droit d'auteur, protection des marques…).

Les échanges électroniques (courriers, forums de discussion, etc.) se doivent de respecter la correction normalement attendue dans tout type d'échange tant écrit qu'oral.

La transmission de données classifiées [9] est interdite sauf dispositif spécifique agrée et la transmission de données dites sensibles doit être évitée ou effectuée sous forme chiffrée.

(c) Émission et réception des messages

L'utilisateur doit faire preuve de vigilance vis-à-vis des informations reçues (désinformation, virus informatique, tentative d'escroquerie, chaînes…).

L'utilisateur doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages.

Il 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.

(d) Statut et valeur juridique des messages

D'après la loi[10], l'écrit électronique a la même force probante que l'écrit sur support papier, les messages électroniques échangés avec des tiers peuvent donc, au plan juridique, former un contrat.

L'utilisateur doit, en conséquence, être vigilant sur la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels.

---

8 Pour exemple, les messages comportant les termes ("privé") dans l'objet ou sujet du message

9 Il s'agit des données classifiées de défense qui couvre le « confidentiel défense », le « secret défense » et le « très secret défense »

10 Articles 1366-1367 du code civil (Ordonnance n°2016-131 du 10 février 2016 - art. 4)

(e) Stockage et archivage des messages

Chaque utilisateur doit organiser et mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve.

Section VI.2 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 l'établissement.

Internet est un outil de travail ouvert à des usages professionnels (administratifs, pédagogiques ou de recherche). Si une utilisation résiduelle privée, telle que définie en section III.1, peut être tolérée, il est rappelé que les connexions établies grâce à l'outil informatique mis à disposition par l'établissement sont présumées avoir un caractère professionnel.

(a) Publication sur les sites Internet et Intranet de l'établissement

Toute publication d'information sur les sites Internet ou Intranet de l'établissement[11] doit être validée par un responsable de site ou responsable de publication nommément désigné.

Aucune publication d'information à caractère privé (pages privées …) sur les ressources du système d'information de l'établissement n'est autorisée, sauf disposition particulière précisée dans un guide d'utilisation établi par le service ou l'établissement.

(b) Sécurité

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.

Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'établissement. Des règles de sécurité spécifiques peuvent être précisées, s'il y a lieu, dans un guide d'utilisation établi par le service ou 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 VI.3 Téléchargements

Tout téléchargement ou copie de fichiers (notamment sons, images, logiciels, cours en ligne…) sur Internet ou localement doit s'effectuer dans le respect des droits de propriété intellectuelle tels que définis à l'article VIII.

L'établissement se réserve le droit de limiter le téléchargement ou la copie de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information (virus, codes malveillants, programmes espions …).

Article VII. Traçabilité

L'établissement est dans l'obligation légale de mettre en place un système de journalisation[12] des accès Internet, de la messagerie et des données échangées.

L'établissement se réserve le droit de mettre en place des outils de traçabilité sur tous les systèmes d'information.

L'établissement s'est doté d'une « politique générale de gestion des journaux informatiques », inscrite au registre informatique et libertés de l'établissement. Elle mentionne notamment les conditions et la durée de conservation des traces de connexions ou d'utilisation des services, et les modalités d'expression du droit d'accès dont disposent les utilisateurs, en application de la loi informatique et libertés du 6 janvier 1978 modifiée et du Règlement général européen (UE) 2016/679 sur la protection des données (RGPD).

11 A partir des ressources informatiques mises à la disposition de l'utilisateur.
12 Conservation des informations techniques de connexion telles que l'heure d'accès, l'adresse IP de l'utilisateur…

Article VIII. Respect de la législation sur les données personnelles

L'utilisateur a l'obligation de respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel, conformément à la loi n° 78-17 du 6 janvier 1978 modifiée dite « Informatique et Libertés » et du Règlement général européen (UE) 2016/_679 sur la protection des données (RGPD).

Les données à caractère personnel sont des informations susceptibles d'identifier directement ou indirectement et par quelque moyen que ce soit les personnes physiques auxquelles elles se rapportent.

Toutes les créations de fichiers comprenant ce type d'informations et demandes de traitement afférent, y compris lorsqu'elles résultent d'extraction, de croisement ou d'interconnexion de fichiers préexistants, sont soumises aux obligations légales et doivent avoir fait l'objet d'une instruction préalable par le délégué à la protection des données (DPD) de l'établissement.

Par ailleurs, conformément aux dispositions légales, chaque utilisateur dispose de droits relatifs aux données le concernant, y compris les données portant sur l'utilisation des systèmes d'information : information, consentement, opposition, limitation, accès, rectification, portabilité, oubli, notification de violation de données, contestation d'une décision automatique, droit à réparation.

Ces droits peuvent s'exercer auprès du délégué à la protection des données (DPD) de l'établissement.

Article IX. Respect de la propriété intellectuelle

L'établissement rappelle que l'utilisation des ressources informatiques[13] 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 X. Limitation des usages

En cas de non-respect des règles définies dans la présente charte et des modalités définies dans les guides d'utilisation établis par le service ou l'établissement, la « personne juridiquement responsable » de l'établissement pourra, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des utilisateurs, limiter les usages par mesure conservatoire.

Par « personne juridiquement responsable », il faut entendre toute personne ayant la capacité de représenter l'établissement (président d'université, directeur d'institut…).

Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extra-professionnelles est passible de sanctions.

Article XI. Entrée en vigueur de la charte

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

Il est annexé au règlement intérieur.

13 Y compris les ressources pédagogiques.

Annexe

Principales références légales

(a) Infractions prévues par le Nouveau Code pénal

Crimes et délits contre les personnes

Atteintes à la personnalité : (Respect de la vie privée art. 9 du code civil)

- Atteintes à la vie privée (art. 226-1 al. 2 ; 226-2 al. 2, art.432-9 modifié par la loi nº2004-669 du 9 juillet 2004) ; atteintes à la représentation de la personne (art. 226-8)
- Dénonciation calomnieuse (art. 226-10)
- Atteinte au secret professionnel (art. 226-13)
- Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques (art. 226-16 à 226-24, issus de la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Atteintes aux mineurs : (art. 227-23 ; 227-24 et 227-28).

- Loi 2004- 575 du 21 juin 2004 (LCEN)

Crimes et délits contre les biens

- Escroquerie (art. 313-1 et suite)
- Atteintes aux systèmes de traitement automatisé de données (art. 323-1 à 323-7 modifiés par les lois nº 2004-575 du 21 juin 2004 et n°2015-912 du 24 juillet 2015).

Cryptologie

- Art. 132-79 (inséré par loi nº 2004-575 du 21 juin 2004 art. 37)

(b) Infractions de presse (loi 29 juillet 1881, modifiée)

- Provocation aux crimes et délits (art.23 et 24)
- Apologie des crimes contre l'humanité, apologie et provocation au terrorisme, provocation à la haine raciale, « négationnisme » contestation des crimes contre l'humanité (art. 24 et 24 bis)
- Diffamation et injure (art. 30 à 33)

(c) Infraction au Code de la propriété intellectuelle

- Contrefaçon d'une œuvre de l'esprit (y compris d'un logiciel) (art. 335-2 modifié par la loi nº 2004-204 du 9 mars 2004, art. 34 - et art. 335-3)
- Contrefaçon d'un dessin ou d'un modèle (art. L521-4 modifiée par la loi nº 2004-204 du 9 mars 2004, art. 34)
- Contrefaçon de marque (art. L716-9 - modifié par la loi nº 2004-204 du 9 mars 2004, art.34 -et suivants)

Il est rappelé que cette liste n'est qu'indicative et que la législation est susceptible d'évolution.

L'informatique à Pagora

Ce document s'adresse aux élèves de Grenoble INP - Pagora, UGA **Mise à jour du 04/06/2026**

Sommaire

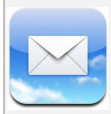

La charte


Les salles


Vos identifiants


Vos données


Les sauvegardes


La messagerie


Les copieurs MFP


WiFi /VPN

Ce document vous explique le fonctionnement du système informatique à Pagora. Il est en ligne sur l'intranet : **https://intrapagora.grenoble-inp.fr**

Le service informatique est composé de :

Franck MONDIN

Responsable du Service informatique
Bureau **B104**
franck.mondin@pagora.grenoble-inp.fr

Lydia VINSARD

Bureau **B103 – les après-midi**
lydia.vinsard@pagora.grenoble-inp.fr

Pour nous joindre par mail :

pagora.sinfo@grenoble-inp.fr

L'informatique à Pagora

Ce document s'adresse aux élèves de Grenoble INP - Pagora, UGA **Mise à jour du 04/06/2026**

Sommaire


La charte


Les salles


Vos identifiants


Vos données


Les sauvegardes


La messagerie


Les copieurs MFP


WiFi /VPN



La charte

La charte de Grenoble INP - UGA et « **L'Informatique à Pagora** » sont consultables sur :

https://intranet.pagora.grenoble-inp.fr/services/charte-dusage-du-systeme-dinformation-eleves

Vous pouvez retrouver toutes nos informations sur l'intranet de l'École :

https://intranet.pagora.grenoble-inp.fr/services/informatique

Résumé en 7 points :

1 – Vos identifiants sont personnels et strictement confidentiels ;

2 – Vous êtes responsable de vos identifiants et de l'utilisation qui en est faite ;

3 – **Vous ne devez pas utiliser les identifiants d'un autre usager** ou chercher à les connaître et vous ne devez pas les dévoiler à un tiers comme Gmail ou équivalent ;

4 – **Vous ne devez pas laisser votre session en libre accès pour autrui ;**

5 – Votre adresse mail de structure de type **Prenom.Nom@grenoble-inp.org** sera la seule adresse mail utilisée pour communiquer entre vous et les différents services de Pagora (Scolarité, Direction des Études, etc.) ;

6 – Vous devez respecter la correction normalement attendue dans tout type d'échange tant écrit qu'oral pour vos échanges électroniques ;

7 – Vous êtes informés que Grenoble INP, UGA et Pagora – LGP2, UGA sont dans l'obligation légale de mettre en place un système de journalisation des accès Internet, de la messagerie et des données échangées.

L'informatique à Pagora

Ce document s'adresse aux élèves de Grenoble INP - Pagora, UGA **Mise à jour du 04/06/2026**

Sommaire


La charte


Les salles


Vos identifiants


Vos données


Les sauvegardes


La messagerie


Les copieurs MFP


WiFi /VPN



Les salles informatiques

Pagora dispose de **6** salles informatiques réparties comme suit :

- Salle **B110** : 12 postes en Windows 11, en libre-service en dehors des enseignements
- Salle **B111** : 20 postes en Windows 11, en libre-service en dehors des enseignements
- Salle **B113** : 12 postes en Windows 11, en libre-service en dehors des enseignements
- Salle **B127** : 18 postes en Windows 11, **Labo. de langue**, en libre-service en dehors des enseignements
- Salle **C102** : 10 postes en Windows 11, en libre-service en dehors des enseignements
- Salle **C103** : 10 postes en Windows 11, en libre-service en dehors des enseignements

1 – Il n'est pas autorisé de pénétrer dans les salles avec de la nourriture et/ou des boissons - les gobelets & bouteilles doivent rester dans les sacs ;

2 – Les salles sont accessibles de 7h30 à 18h45 maximum ;

3 – Vous ne devez en aucun cas débrancher les câbles d'alimentation électrique ou réseau par mesure de sécurité et de bon fonctionnement des ordinateurs ;

4 – Vous ne devez pas utiliser les ordinateurs comme des consoles de jeux ou des téléviseurs. **Les activités ludiques ne sont pas autorisées** ;

5 – Vous **devez signaler tout dysfonctionnement** dans les plus brefs délais, par mail à **pagora.sinfo@grenoble-inp.fr** ou aux bureaux B104/B103 muni du nom (indispensable) de la machine concernée (**PAGORA-Fxxxx**) ;

6 – En partant, vous devez **veiller à ce que votre session se ferme normalement au risque d'un « profil » cassé.** Laisser votre place propre ; des poubelles sont à votre disposition dans chaque salle. Vérifiez que vous **n'oubliez rien, surtout votre clé USB !** Merci de déposer celles que vous trouvez à la Scolarité ou au Sce Informatique, une autre fois, ce pourrait être la vôtre.

INFORMATION : La suite ADOBE CC est installée en **C102** et **C103**.
Lors de l'ouverture d'un des logiciels, vous devez créer – ou utiliser - un compte ADOBE avec votre adresse mail académique.

L'informatique à Pagora

Ce document s'adresse aux élèves de Grenoble INP - Pagora, UGA **Mise à jour du 04/06/2026**

Sommaire


La charte


Les salles


Vos identifiants


Vos données


Les sauvegardes


La messagerie


Les copieurs MFP


WiFi /VPN



Vos identifiants TRIODE

Vos identifiants servent à ouvrir une session sur n'importe quel ordinateur de Pagora et permettent d'accéder aux différents sites Web de Grenoble INP, UGA ;

En particulier, vous pouvez accéder à votre emploi du temps (**ADE**) comme suit : **https://edt.grenoble-inp.fr/2026-2027/etudiant/pagora**

1 – Une **lettre** vous est fournie en début d'année, remise en main propre ; elle contient votre identifiant utilisateur, votre login de messagerie, un éventuel code d'initialisation du mot de passe et votre code personnel à 8 chiffres pour les copieurs multifonctions.

Conservez-la bien ainsi que ce document pour toutes les informations qu'ils contiennent.

Vos identifiants sont strictement **personnels** et **confidentiels**.

2 – Le coffre-fort de mots de passe "CoPass" :

Si un *code d'initialisation du mot de passe* est mentionné dans votre lettre, allez sur **https://copass-client.grenet.fr** , saisissez-*le* dans la case « Code Inscription » et suivez les instructions pour définir votre mot de passe.

→ À tout moment (FR / ENG) : **https://copass-client.grenet.fr/#/aide**

ATTENTION : N'oubliez pas votre nouveau mot de passe, il vous sera nécessaire pour l'accès à de multiples ressources numériques.

3 – En cas de **perte** ou de **vol** de vos codes, **il est obligatoire** de le signaler immédiatement à un des membres du service informatique (M. MONDIN en B104 / Mme VINSARD en B103) afin que vos comptes ne soient pas usurpés.

En tant qu'étudiant, vous pouvez retrouver vos accès en autonomie via le copass-client (https://copass-client.grenet.fr/#/reinitialiser-le-mot-de-passe). Le système vous envoie un code sur l'adresse personnelle fournie lors de votre inscription.
Vous pouvez également « renvoyer votre mot de passe » pour le repropager.

L'informatique à Pagora

Ce document s'adresse aux élèves de Grenoble INP - Pagora, UGA **Mise à jour du 04/06/2026**

Sommaire


La charte


Les salles


Vos identifiants


Vos données


Les sauvegardes


La messagerie


Les copieurs MFP


WiFi /VPN



Vos données

Vos données doivent être enregistrées sur le lecteur réseau « **TravailPerso (T:)** ».
Vous disposez d'un espace de stockage de 5 Giga octets.

Vous bénéficiez d'un **profil** dit « **itinérant** » lorsque vous vous connectez aux ordinateurs Windows de l'école, c'est à dire que votre environnement vous « suit » lorsque vous changez de poste de travail.
Il contient vos favoris internet, votre bureau, fond d'écran …

Privilégiez les raccourcis.

Un profil itinérant peut être chargé de fichiers temporaires et empêcher la fermeture de votre session. Dans ce cas, supprimer des fichiers dans votre profil afin de pouvoir fermer votre session normalement.

Vous pouvez **provisoirement** créer un sous-répertoire (de préférence *à votre nom ou nom de connexion*) dans « Temp » dans « **General (G:)** » afin de déposer un travail effectué en groupe ou en vue d'un échange de fichier(s).

La durée de conservation de ces fichiers est de 10 jours.

L'informatique à Pagora

Ce document s'adresse aux élèves de Grenoble INP - Pagora, UGA **Mise à jour du 04/06/2026**

Sommaire


La charte


Les salles


Vos identifiants


Vos données


Les sauvegardes


La messagerie


Les copieurs MFP


WiFi /VPN



Les sauvegardes

Vos données sur **T:** sont sauvegardées 1 fois par jour. Après suppression d'un fichier ou d'un dossier, vous disposez de 30 jours maximum pour le restaurer.

Attention ! Le système de sauvegarde n'est pas infaillible : bien qu'il y ait 2 types de sauvegardes distincts, veillez également à sauvegarder vos données sur d'autres supports fiables personnels.

Rappel : la clé USB n'est pas un support fiable !

Dicton informatique :
« *Si la donnée existe une fois, c'est comme si elle n'existait pas !* »

L'informatique à Pagora

Ce document s'adresse aux élèves de Grenoble INP - Pagora, UGA **Mise à jour du 04/06/2026**

Sommaire


La charte


Les salles


Vos identifiants


Vos données


Les sauvegardes


La messagerie


Les copieurs MFP


WiFi /VPN



La messagerie

Pour accéder à votre messagerie, utiliser un navigateur WEB et connectez-vous comme suit :

https://webmail.grenoble-inp.org

1 – **Pour vous connecter** :

login court
mot de passe défini par vos soins

Les différents services de Pagora et plus généralement Grenoble INP vous écriront uniquement à cette adresse ! Vous devez vous-même correspondre avec cette adresse dans le cadre de votre scolarité ;

2 – Vous devez **relever** votre messagerie **régulièrement** et faire le ménage afin que votre boîte mail ne soit pas saturée (**1 Go** alloué). Vérifiez aussi les « Spams » ;

3 – **Listes de diffusion** : une liste de diffusion vous permet d'écrire à un groupe d'individus ; les listes de diffusion sont soumises à des règles.
Vous faites partie de certaines listes de diffusion avec modérateur auxquelles vous ne pouvez pas vous désabonner (ex : listes de la Scolarité), et d'autres desquelles vous pourrez éventuellement vous désabonner ;

Pour atteindre vos correspondants, **n'utilisez pas** la forme [LISTE]**-request** (**-request** correspond à une demande au support de la liste, sauf si c'est le but) :
https://listes-pagora.grenoble-inp.fr/sympa

4 – Pour joindre le **support Zimbra étudiants** : simsu-service-mail-etudiants-partage-inp@grenet.fr ; il n'y a pas de sauvegarde de la messagerie, elle est externalisée.

5 – Configuration de la messagerie avec un **client « lourd »** (ex. : Thunderbird) ou pour consultation via un logiciel de messagerie sur smartphone / PC / tablette :

login : **prenom.nom@grenoble-inp.org**
mot de passe

IMAP : imap.grenoble-inp.org port 993 en SSL
SMTP : smtp.grenoble-inp.org port 587 en STARTTLS

ATTENTION : il est interdit de relever cette boite via Gmail, Yahoo ou autre messagerie web, car dans ce cas, vous communiqueriez vos identifiants personnels et confidentiels à un tiers. Ceci est interdit par la charte informatique que vous signez en début d'année universitaire.

L'informatique à Pagora

Ce document s'adresse aux élèves de Grenoble INP - Pagora, UGA **Mise à jour du 04/06/2026**

Sommaire


La charte


Les salles


Vos identifiants


Vos données


Les sauvegardes


La messagerie


Les copieurs MFP


WiFi /VPN



Les copieurs multifonctions (MFP)

Le matériel

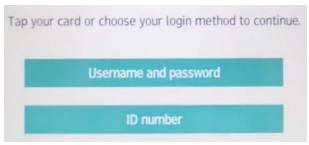
Pagora dispose de **6** copieurs MFP répartis comme suit :

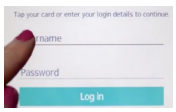
- Copieur **Noir&Blanc** « RICOH MP 5055 » **(Pagora-NInfo)** au 1er étage du bâtiment « B » vers B113 : 50 pages par minute (ppm) ; A4/A3 ; agrafage possible ; **port USB local activé**

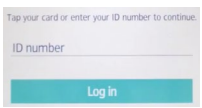
→ N'oubliez pas de votre clé USB en partant

- Copieur **Couleur** « RICOH IM C3000 » **(Pagora-CBatBEt)** au 1er étage du bâtiment « B » vers B117 : 30 ppm ; A4/A3 ; agrafage possible
- Copieur **Couleur** « RICOH IM C3000 » **(Pagora-CBatBRc)** au rez-de-chaussée du bâtiment « B » vers B019 : 30 ppm ; A4/A3 ; agrafage possible
- Copieur **Couleur** « RICOH IM C3000 » **(Pagora-CImp)** au 1er étage du bâtiment « C » vers C103 : 30 ppm ; A4/A3 ; agrafage possible
- Copieur **Couleur** « RICOH IM C3000 » **(Pagora-CBib)** à la bibliothèque (1er étage, salle D102) : 30 ppm ; A4/A3 ; agrafage possible
- Copieur **Couleur** « RICOH IM C3000 » **(Pagora-CAdm)** au 1er étage du bâtiment « D » vers D105 : 30 ppm ; A4/A3 ; agrafage possible (**interdit aux élèves**)

3 possibilités d'authentification









- ✓ Vous disposez d'un code utilisateur à 8 chiffres.
- ✓ Vous pouvez utiliser votre login et votre mot de passe TRIODE.
- ✓ Vous avez associé votre carte d'étudiant au lecteur de badge des copieurs.

→ N'oubliez pas de vous déconnecter à chaque fois et surveillez votre solde !

L'informatique à Pagora

Ce document s'adresse aux élèves de Grenoble INP - Pagora, UGA **Mise à jour du 04/06/2026**

Sommaire


La charte


Les salles


Vos identifiants


Vos données


Les sauvegardes


La messagerie


Les copieurs MFP


WiFi /VPN



Les impressions, photocopies & scans

Les copieurs multifonctions sont tous configurés en NB et RECTO-VERSO **par défaut** dans le respect du cadre environnemental.

Les copieurs couleur distinguent les pages NB (**aucun** pixel en couleur dans la page) des pages avec couleur lors de vos demandes d'impression en couleur, mais vérifiez bien toujours le montant calculé par l'outil **PaperCut**.



Les impressions



1 – Ouvrez votre document et cliquez sur imprimer ;
– Choisissez l'imprimante virtuelle « **pagora-impression-eleves** » (par défaut) ;
– Un message du logiciel **PaperCut** vous indique le coût de votre impression ;
– Vérifiez puis validez votre demande si elle vous convient, sinon annulez.

ATTENTION : **si le calcul vous semble faux ou qu'il n'aboutit pas, annulez votre demande et rapprochez-vous du Service Informatique.**

2 – Dirigez-vous vers le copieur de votre choix, « couleur » si vous avez demandé une impression en couleur ;
– Authentifiez-vous (voir page précédente) et choisissez « libérer impression » ;
– La liste de vos travaux s'affiche : sélectionner le(s) document(s) que vous souhaitez imprimer. *Les travaux d'impression sont effacés automatiquement de la liste au bout de 72h d'attente ;*

L'informatique à Pagora

Ce document s'adresse aux élèves de Grenoble INP - Pagora, UGA **Mise à jour du 04/06/2026**

Sommaire


La charte


Les salles


Vos identifiants


Vos données


Les sauvegardes


La messagerie

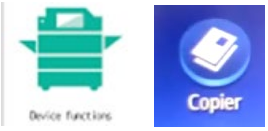

Les copieurs MFP


WiFi /VPN



Les impressions, photocopies & scans

Les photocopies



1 – Connectez-vous selon une des 3 façons expliquées page 8 ;

2 – Sélectionnez « Fonctions périphérique », puis, à l'écran suivant, le symbole « Copie » : vous êtes en mode photocopieur (attention aux options par défaut) ;

3 – Une fois vos travaux terminés, veillez à vous **déconnecter** (en haut à droite).

ATTENTION ! Vous pouvez passer en solde négatif. Tout solde négatif sera dû.

Les Scans To Mail (STM)



1 – Connectez-vous selon une des 3 façons expliquées page 8 ;

2 – Sélectionnez « Numérisation » : vous êtes en mode Scan To Mail (les documents scannés seront envoyés directement dans votre messagerie Grenoble INP) ;

3 – Accepter les paramètres par défaut, sinon modifiez-les à votre convenance pour la session en cours ;

4 – Une fois vos travaux terminés, veillez à vous **déconnecter** (en haut à droite).

Comment créditer son compte

Le coût à la page A4 est de **0,053 € en NB** et **0,218 € en couleur** (tarifs 09/18).

Vous pouvez créditer votre compte d'une somme de 10 à 30 euros avec report d'une année à l'autre *(cas particuliers : CFA / 3e année / PFE au LGP2)*
→ en espèces (**prévoyez l'appoint**)
→ ou par chèque (que vous **DEVEZ préparer à l'avance**, à l'ordre de « **agefpi** »)

aux bureaux B103 / B104 **entre 10h et 10h15** ou **entre 14h45 et 15h**

sous réserve de disponibilité des membres du Service Informatique.
Si possible, anticipez 😉**, merci**

L'informatique à Pagora

Ce document s'adresse aux élèves de Grenoble INP - Pagora, UGA **Mise à jour du 04/06/2026**

Sommaire


La charte


Les salles


Vos identifiants


Vos données


Les sauvegardes


La messagerie


Les copieurs MFP


WiFi / VPN

Le WiFi et le VPN

- 2 réseaux wifi sont à votre disposition au sein de l'école :
  wifi-campus & **EDUROAM**
- Vous pouvez trouver des informations sur le nomadisme au sein de la communauté Université Grenoble Alpes sur :

https://intranet.grenoble-inp.fr/systeme-d-information-numerique/outils-et-applications/nomadisme-wifi

1 – wifi-campus (*basique mais ouvert aux visiteurs*) **:**

https://intranet.grenoble-inp.fr/systeme-d-information-numerique/outils-et-applications/wifi-campus

Pour vous connecter, choisissez le réseau « **wifi-campus** », puis ouvrez votre navigateur Web : vous serez automatiquement redirigé vers le portail WiFi afin de vous identifier en sélectionnant votre établissement de rattachement et en mentionnant votre nom d'utilisateur et le mot de passe associé.

→ Lisez attentivement la charte avant d'accepter d'utiliser ce service.

2 – EDUROAM (*transparent, mondial mais limité*) **:**

Documentation :
https://intranet.grenoble-inp.fr/systeme-d-information-numerique/outils-et-applications/eduroam

Vous avez aussi la possibilité de vous connecter au réseau « **EDUROAM** » :

– Renseignez l'identifiant sous le format **login@grenoble-inp.fr** et utilisez votre mot de passe habituel.

3 – VPN

https://intranet.grenoble-inp.fr/systeme-d-information-numerique/outils-et-applications/vpn

Le VPN est indispensable pour se connecter à **RefEns** depuis l'extérieur.

profil : vpn.grenet.fr