Charter Defining the Use of IT Facilities

Institut polytechnique de Grenoble,
Graduate Schools of Engineering and Management,
Université Grenoble Alpes

Index

Preamble

The following translation is for information only and has no contractual value.

The phrase 'IT facilities' refers to all the data, hardware, software, applications, databases and local telecommunication network resources, as well as all resources which enable remote or transitive access from the network of Institut polytechnique de Grenoble, Graduate Schools of Engineering and Management, Université Grenoble Alpes.

It also encompasses mobile computing facilities, such as personal digital assistants, portable computers and mobile phones.

The term "user" refers to any person entitled to a computer account or having access to the IT facilities regardless of status.

Notably, this refers to:

- *Any staff, irrespective of his or her contract, fulfilling an assignment coming under the provision of public service in the fields of teaching or research;*
- *Any student enrolled in the Establishment;*
- *Any person exterior to the Establishment, visitor, guest, or person under contract[1] to the Establishment.*

Proper operation of the IT facilities requires compliance with the legislative and regulatory requirements, notably compliance with rules concerning security, operation procedures and data storage.

This chapter defines the rules of use and security with both the Establishment and user agree to comply with. It specifies the rights and duties of each party.

Responsibilities of the Establishment

The Establishment must inform the user of the charter.

The Establishment must take all necessary measures to ensure the security of the IT facilities and the protection of users.

The Establishment must facilitate user access to the resources available via the IT facilities. Although the resources available are for professional usage the Establishment must respect the residual use of IT resources in a personal capacity.

Responsibilities of the User

The user is responsible, at all times, for the usage which he or she makes of the available IT facilities. He/she has an obligation of confidentiality with regard to the information and documents he/she produces or accesses. This responsibility implies the respect of rules concerning professional ethics and confidentiality.[2]

In any case, the user shall comply with the requirements associated with his or her position or contract.

The available resources must be used appropriately and in good faith so as to avoid hindering the performance of the IT facilities and abusive use of resources for personal ends.

Article I. Scope

The security rules and terms of use defined in the Charter apply to the Establishment and all of its users.

The use of IT facilities related specifically to the activity of union organisations is not covered by the Charter.

1 Compliance with the Charter must be explicitly stated as an obligation within the contract.
2 In particular, patient confidentiality in health related fields.

These rules apply to any person authorised to use any of the computer facilities of the Establishment, including off-site and shared computer facilities, and covers external networks accessible through Establishment networks.

Article II. Right of Access to IT Facilities

Right of access to IT facilities is temporary. Access will be withdrawn if no longer justified by the situation of the user and, unless specifically requested, will be withdrawn within 3 months of the expiration of a user's computer account entitlement.

It may also be withdrawn, as a precautionary measure, if the behaviour of a user is incompatible with the rules as specified in the Charter.

Article III. Data protection and privacy

The user is responsible for his or her professional data, or that to which he or she has access in the scope of his or her duties. In particular, he/she must ensure that his/her data are backed up and that he/she is vigilant about the access rights it gives to other users.

The user must ensure the protection of sensitive information (for which a direct or indirect requirement for confidentiality has been identified); in particular, he/she must avoid communicating or transporting it without protection (encryption) via insecure media (messaging, USB keys, laptops, external disks, etc.) and must not place it on a external server or available to the general public.

Article IV. Conditions of Use of IT Facilities

Section IV.1 Professional vs. Private Use

Use of the IT facilities of the Establishment exclusively covers purposes of research, teaching, documentation, administration or other aspects of university activity. Unless authorised, these systems cannot be used for the operation of projects which are not associated to the Establishment or to projects assigned to the user. They may, however, be used for private communication under the conditions described below.

Residual usage of the IT facilities for private use must be for non-profit activities and moderate in terms of frequency, volume and duration. Whatever the case, the additional resulting costs must be negligible in comparison to the overall operation costs.

This usage must not have a negative effect on the quality of work provided by the user, on the time the user dedicates to his or her working duties or to the proper functioning of the Establishment.

All information is considered professional with the exclusion of data explicitly designated by the user, as relative to his or her private life, regardless of the medium (computers, USB sticks, phones, etc.) or the service used (storage space, messaging, etc.).

Thus, it is the responsibility of the user to store data of a private nature in an appropriate area dedicated explicitly[3] for this purpose or to indicate the private nature of the data on the resource[4]. The user is responsible for the protection and backup of private data.

The user is responsible for his or her private data space. Upon his or her departure from the Establishment, it is his or her responsibility to delete his or her private data space. The Establishment does not have the duty to maintain this space. Data conservation measures of professional data are defined by the person deemed responsible by the Establishment. In the case of the death of a user, his or her private space will be deleted.

Private usage of the IT facilities must respect the applicable laws.

In particular, the storage, dissemination or exporting of images of a paedophile nature, or the

3 For example, this space may be named "_private_" or "_prive_"
4 For example, "_private_name_of_object": the object may be a message, a file or any other digital resource.

dissemination of anti-Semitic or racist material[5] is strictly forbidden.

Additionally, in character with the aims of the Establishment, consultation of sites of a pornographic nature within the grounds of the Establishment, outwith a professional context, is forbidden[6]

Section IV.2 Maintenance of Departmental Operations in Case of Absence and Departure

In order to maintain departmental operations, the user should make every effort to store files in the areas shared by the members of his or her department or work group. In any case, any data not situated in the space identified as private will be considered as belonging to the Establishment that will be able to have unrestricted access.

In the case of departure or prolonged absence, the user must inform his or her hierarchy of the procedures allowing access to the resources made specifically available to him or her. These procedures shall comply with the safety rules set out in Section V. 1.

Article V. Security principle

Section V.1 Applicable Security Rules

The Establishment will take appropriate security measures for the IT facilities available to users.

The user will be informed that access codes constitute one of the security measures aimed at avoiding malicious or abusive use. However, this security measure does not imply that information tools protected in this way are of a personal nature.

The levels of access granted to the user depend upon the tasks assigned to the user. The security of the IT facilities available requires that the user:

- Follow the security instructions, notably the rules relating to the management of access codes. Each user is responsible for the usage made of their access codes.
- Keep his or her access codes confidential and never share them with a third party.
- Respect the access policy, and in particular, not use the access codes of another user nor attempt to attain them.
- Ensure that he or she never leaves a freely accessible work station unattended.

In addition, the security of the resources available to the user requires several precautions:

✓ On the part of the Establishment:

- Ensure that sensitive information is only accessible to the persons concerned. Exceptions may be made for practices concerning organisation of departmental operation continuity, as decided by the relevant hierarchy.
- Limit the access of the user to only the information for which he or she has been explicitly allowed.

✓ On the part of the user:

- Ensure that he or she does not access or attempt to access resources available via the IT facilities for which he or she has not been explicitly granted permission.
- Ensure that he or she does not connect devices directly to the local network other than those authorised by the establishment or those detailed in a user guide defined by a department or the Establishment.
- Ensure that he or she does not install, download or use software without the required license or originating from untrustworthy sources or without the authorisation of the Establishment.

5 Article 24 and 26 *bis* of *Loi du 29 juillet 1881*.
6 *Code Pénal* (Penal Code), article L 323-1 and subsq. articles.

- Follow the guidelines defined by the Establishment concerning viruses and computer program attacks.
- Ensure that he or she does not intentionally jeopardise the smooth operation of the computer resources and networks by abnormal usage of hardware or software.
- Make all efforts to safeguard the equipment made available to him or her against theft of or damage.
- Apply any security recommendations issued by the Establishment.

Section V.2 Notification Obligations

The user must notify the person responsible for the security of IT facilities of any irregularity, such as a security breach, as soon as possible. He or she must also notify his or her superior or the hierarchy of any access to a resource which does not correspond to his or her status.

Section V.3 Control and Monitoring Policy

The user shall be provided with the following information:

- Procedures for corrective, curative or adaptive maintenance. The establishment reserves the right to perform maintenance (remotely if necessary) upon any resources provided.
- The user will be informed of any remote maintenance prior to its occurrence.
- Any information blocking the operation of IT facilities or causing disruption through its delivery, will be quarantined and if necessary deleted.
- The IT facilities, within the boundaries of the applicable legislation, may be subjected to the following: surveillance or testing measures for statistical purposes; traceability measures for legal or functional requirements; optimisation; security measures; detection of abusive behaviour measures.

The personnel responsible for the control operations of IT facilities are bound by professional confidentiality. They are not permitted to divulge any information which they may encounter as part of their functions given the following circumstances:

- The information is covered by correspondence confidentiality or, being identified as such, is private information of the user.
- The information does not jeopardise the proper operation of applications or their security.
- The information does not fall under article[7] 40, paragraph 2 of the *Code de Procédure Pénale* (Code of Criminal Procedure).

Article VI. Electronic Communication

Section VI.1 Emailing

The use of emails constitutes one of the essential elements for work optimisation, the sharing of means and resources and the exchange of information within the Establishment.

(a) Email Addresses

The Establishment will provide the user with a nominative professional email address for sending and receiving email. Once assigned, use of this nominative address will be under the responsibility of the user.

This nominative email address is merely an extension of the administrative address and does not diminish the professional nature of the messaging system in any way.

7 The obligation of every civil servant to notify as soon as possible the *Procureur de la République* of any crime or misdemeanour of which he or she becomes aware as a result of their employment.

An email address related to a position or organisation-entity, can be created for a user or group of users when required by the Establishment.

The management of email addresses corresponding to institutional mailing lists designating a category or group of "users" is the exclusive responsibility of the Establishment. Such lists can only be used by authorised users.

(b) Email Content

Every message will be considered as professional unless explicitly referenced as being of a private nature[8] or stocked in the private data storage area.

In order to maintain correct departmental operations, limitations may be implemented. In particular, reduction methods for undesirable messages (such as spam and viruses) may be put in place.

Messages containing content of an illicit nature are forbidden. Notably, this applies to content that contravenes the legal regulations on the freedom of expression and privacy (such as, jeopardizing an individual's peace of mind through threatening behaviour or defamation, damaging an individual's honour through non-public personal insult and breaches of copyright or the proprietary rights of a business).

All forms of electronic exchange (email, forums, etc.) must respect the accepted forms of normal behaviour applicable to any type of exchange, whether written or oral.

The transmission of classified data[9] is forbidden without specific authorisation and the transmission of sensitive data, when unavoidable, must be sent in an encrypted format.

(c) Sending and Receiving Emails

The user must exercise vigilance regarding information received (disinformation, computer viruses, scams, chain letters, etc.).

The user must verify the identity and correctness of the address of a potential recipient of a message.

The user must ensure that the diffusion of messages be limited only to those concerned by its contents so as to avoid mass mailing, over-encumbered email accounts and an overall degradation of service.

(d) Legal Status of Messages

According to the law, digital writing has the same probative value as paper-based writing, so electronic messages exchanged with third parties can legally represent a contract.

The exchange of emails with third parties can, from a legal point of view, represent a contract, under the conditions specified in sections[10] 1369-1 to 1369-11 of the *Code Civil* (Civil Law Code).

Consequentially, the user must attach the same importance to the nature of electronic messages as to traditional correspondence.

(e) Storing and Archiving of Messages

Each user must employ the necessary methods for the conservation of messages which may be indispensible or even merely useful as evidence of a particular activity.

Section VI.2 Internet

It should be noted that the Internet is subject to the totality of applicable law. Use of the Internet (and by extension the intranet) is one of the essential elements for work optimisation, sharing and information accessibility within and outwith the establishment.

The Internet is made available as a work tool for professional purposes (administrative, pedagogical or research). Residual private usage, such as defined in section III.1, may be tolerated but it should be noted

8 For example, messages containing the terms ("private" or "prive") in the subject of the message.
9 This term refers to classified defence data which covers *confidentiel défense*, *secret défense* and *très secret défense* data.
10 Articles 1366-1367 of the Civil Law Code (Ordinance n°2016-131 of 10 February 2016 - art. 4)

that connections established using resources provided by the establishment are presumed to be of a professional nature.

(a) Publication on Establishment Websites or Intranets

Any publication of information on an Internet or intranet site belonging to the Establishment[11] must be approved by the person responsible for the site or the person, explicitly named, responsible for publication.

The publication of information of a private nature (such as a private site) using the IT facility resources belonging to the Establishment is forbidden, unless specifically authorised as defined in a user guide issued by the department or Establishment.

(b) Security Policy

The Establishment reserves the right to restrict or forbid access to certain sites and to perform surveillance, either before or after the fact, of sites visited and the duration of access.

Access is authorized solely in so far as it complies with the security procedures set up by the Establishment. Additional security procedures may be requested and defined in a user guide issued by a department or by the Establishment.

The user is informed of the inherent risks and limitations regarding use of the Internet through training and awareness programs.

Section VI.3 Downloading Policy

Any downloading or copying of files (notably sound files, images, software and online courses) on the Internet or locally must comply with intellectual property rights as defined in Article VII.

The Establishment reserves the right to limit the downloading or copying of certain files on the basis of file size or the possibility of security risks to the IT system (viruses, malicious code, spyware, etc.)

Article VII. Traceability

The Establishment is legally obliged to set up a data logging system[12] for Internet access, messaging and data transfers.

The Establishment reserves the right to install data tracking tools on all information systems.

The Establishment has adopted a "general policy for the management of computer logs", entered in the establishment's “informatique et liberté” register. It mentions in particular the conditions and the duration of conservation of the traces of connections or use of services, and the methods of expression of the right of access which the users have, in application of Act No. 78-17 of 6 January 1978 modified and of the European General Data Protection Regulation (GDPR - EU 2016/679).

Article VIII. Compliance with Intellectual Property Rights

The Establishment reminds all users that the use of IT resources[13] implies the respect of its intellectual property rights, those of its partners and more generally, of all third parties holding such rights.

As a consequence, each user must:

- Only use software under the licensing conditions granted;
- Not reproduce, copy, distribute, modify or use software, databases, web pages, texts, images, photographs or other creative content protected by creative or exclusive rights, without having first obtained authorisation from the holders of these rights.

11 From utilising the IT resources made available to the user.
12 Storage of technical connection information such as access time, user IP address, etc.
13 Including pedagogical resources.

Article IX. Compliance with Data Protection Act

The user has the obligation to respect the legal provisions as regards automated processing of personal data, in accordance with the law n° 78-17 of January 6, 1978 known as "Loi Informatique et Libertés" (data Protection Act) and of the European General Data Protection Regulation (GDPR - EU 2016/679).

Personal data is information which – in whatever form – makes in possible to identify, either directly or indirectly, the physical person to whom it applies.

The creation of a file containing this type of information and related processing requests, including when they result from extraction, cross-referencing or interconnection of pre-existing files, are subject to legal obligations and must have been the subject of an instruction by the Data Protection Officer (DPO) of the Establishment.

In addition, in accordance with legal provisions, each user has rights relating to the data concerning him, including data relating to the use of information systems: information, consent, limitation, access, rectification, deletion, portability, right to be forgotten, breach notification, contestation of an automatic decision, right to compensation.

Exercises of this right may be handled by the Establishment's Data Protection Officer (DPO).

Article X. Limitation of Access

In the case of contravention of the regulations defined in this document and of the procedures defined in user guides established by departments or the Establishment, the "person legally responsible" for the Establishment may, independently of the legal or disciplinary actions that may be taken against the users, limit access as a precautionary measure.

"Person legally responsible" refers to any person with the capacity to represent the Establishment (university president, institute director, etc.)

Any abuse of resources made available to the user for ends outwith professional usage is open to sanction.

Article XI. Charter Commencement Date

This document annuls and replaces all previous documents or charters relating to the use of the Establishment's IT facilities.

It will be effective in each institution on the date of its approval by the competent authority.

It is an Appendix to the Rules and Policies.

Appendix

Core Legal References

(a) Offences under *Nouveau Code Pénal* (New Penal Code)

Offences against Natural Persons

Offences against personality: (Privacy rights section, art. 9, *Code Civil* -Civil Law Code)

- Offences against privacy (art. 226-1 paragraph 2 ; 226-2 paragraph. 2, art. 432-9 amended by *Loi nº2004-669 du 9 juillet 2004*); offences against the image of persons (art. 226-8)
- Malicious denunciation (art. 226-10)
- Breach of professional secrecy (art. 226-13)
- Violation of personal rights resulting from computer files or processes (art. 226-16 to 226-24, from *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* and amending *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*)

Offences against Minors: (art. 227-23; 227-24 and 227-28).

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

Offences against Property

- Fraudulent obtaining and similar offences (art. 313-1 and subsq. art.)
- Unauthorised access to automated data processing (art. 323-1 to 323-7 amended by *Loi nº 2004-575 du 21 juin 2004*).

Encryption

- Art. 132-79 (added to the Code by *Loi nº 2004-575 du 21 juin 2004* art. 37)

(b) Press Offences (*Loi 29 juillet 1881,* amended)

- Incitement to crime (art. 23 and 24)
- Condoning of crimes against humanity, condoning and incitement to terrorism, incitement to racial hatred, denial of crimes against humanity (art. 24 and 24 *bis*)
- Defamation and insult (art. 30 to 33)

(c) Intellectual Property Code Infringements

- Infringement of rights pertaining to works of the mind (software products included) (art. 335-2 amended by *Loi nº 2004-204 du 9 mars 2004,* art. 34 - and art. 335-3)
- Infringement of design rights (art. L521-4 amended by *Loi nº 2004-204 du 9 mars 2004,* art. 34)
- Infringement of trademarks (art. L716-9 – amended by *Loi nº 2004-204 du 9 mars 2004,* art.34 –and subsq. art.)

It should be noted that this list is for information only and subject to change.

L'informatique à Pagora

Ce document s'adresse aux élèves de Grenoble INP - Pagora, UGA — Mise à jour du 30/08/23

Sommaire

Ce document vous explique le fonctionnement du système informatique à Pagora. Il est en ligne sur l'intranet : **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**
Lydia.Vinsard@pagora.grenoble-inp.fr

Pour nous joindre par mail :

pagora.sinfo@grenoble-inp.fr (en général)

pagora.soscopieurs@grenoble-inp.fr (**copieurs**)

L'informatique à Pagora

Ce document s'adresse aux élèves de Grenoble INP - Pagora, UGA **Mise à jour du 30/08/23**

Sommaire

La charte

La charte de Grenoble INP - UGA est disponible **ici** :
https://intranet.pagora.grenoble-inp.fr/services/charte-d-utilisation-du-systeme-d-information

Résumé de la charte 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 30/08/23**

Sommaire

Les salles informatiques

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

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

La Salle **B105** avec ses 7 postes en Windows 10 est **réservée aux chercheurs du LGP2 & divers personnels**, en dehors des réservations occasionnelles faites pour les enseignants dans **ADE**.
Elle ne vous est accessible qu'exceptionnellement, sur demande en B103/B104.

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 30/08/23**

Sommaire

Vos identifiants TRIODE

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 le code pour les copieurs multifonctions.

Conservez-la bien ainsi que ce document pour les informations qu'ils contiennent dont votre code personnel à 8 chiffres pour les copieurs.

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.

↳ **Votre mot de passe doit répondre aux critères de complexité suivants** :
12 caractères minimum avec **au moins un** caractère de chaque type :
→ MAJUSCULE,
→ minuscule,
→ chiffre de 0 à 9,
→ caractère spécial parmi ! @ # $ % & * _ - + = ( ) { } < > / ; : , . | ?

Il ne doit contenir ni nom commun, ni nom propre ; la politique de sécurité des mots de passe refusera une connexion à nos PC si votre mot de passe contient vos Nom / Prénom ou Date de naissance !!!

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

3 – 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 ;
En particulier, vous pouvez accéder à votre emploi du temps (**ADE**) comme suit : **https://edt.grenoble-inp.fr/2023-2024/etudiant/pagora**

4 – Vos identifiants sont strictement personnels et confidentiels ;

5 – 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/simsu/reinitialisation) Mot de passe / Initialiser son mot de passe. Le système envoie un code sur l'adresse personnelle fournie lors de votre inscription.

L'informatique à Pagora

Ce document s'adresse aux élèves de Grenoble INP - Pagora, UGA **Mise à jour du 30/08/23**

Sommaire

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, 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 30/08/23**

Sommaire

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 30/08/23**

Sommaire

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

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) ;

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), **ni le suffixe** @listes-pagora.grenoble-inp.fr

https://listes-pagora.grenoble-inp.fr/sympa

4 – Il n'y a pas de sauvegarde de la messagerie (externalisée ; Mail du **support** Zimbra étudiants : **simsu-service-mail-etudiants-partage-inp@grenet.fr**) ;

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 habituel

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 30/08/23**

Sommaire

Les copieurs multifonctions (MFP)

Le matériel

Pagora dispose de **7** copieurs MFP répartis comme suit :

- Copieur **NB «** RICOH MP 5055 **» (Pagora-NInfo)** au 1er étage du bâtiment « B » vers B113 : 50 ppm ; A4/A3 ; agrafage possible ; port USB local activé
- 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)**
- Copieur **NB «** RICOH MP6002 **» (Pagora-NAdm)** au 1er étage du bâtiment « D » vers D105 : 60 ppm ; A4/A3 ; agrafage / perforation possibles **(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 30/08/23**

Sommaire

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 ;
– 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.**

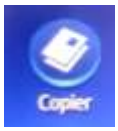
2 – Dirigez-vous vers le copieur de votre choix, « couleur » si vous avez demandé une impression en couleur ;
– Authentifiez-vous (voir page précédente) et choisissez « libérer impression » ;
– La liste de vos travaux s'affiche : sélectionner le(s) document(s) que vous souhaitez imprimer. *Les travaux 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 30/08/23**

Sommaire

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).
Les autres tarifs sont affichés au panneau de liège vers B113.

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** »)

au bureau **B103** / B104 **entre 10h et 10h15** ou **entre 14h45 et 15h**

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

L'informatique à Pagora

Ce document s'adresse aux élèves de Grenoble INP - Pagora, UGA — Mise à jour du 30/08/23

Sommaire

Le WiFi

- 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*) **:**

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

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

1 – Téléchargez l'installeur automatique **https://cat.eduroam.org**

2 – Suivez les instructions à l'écran et veillez à bien choisir « **Institut National Polytechnique de Grenoble** » dans la liste.

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

Avantage : vous restez en permanence connecté au Wi-Fi
Inconvénient : cela diminue l'autonomie de votre appareil

L'informatique à Pagora

Ce document s'adresse aux élèves de Grenoble INP - Pagora, UGA — Mise à jour du 30/08/23

Sommaire

Trucs et astuces

➢ **Votre ordinateur personnel est infecté ?**
Décontaminez-le gratuitement en 4 étapes :

1re étape : téléchargez **ADWCLEANER** via
https://toolslib.net/downloads/viewdownload/1-adwcleaner/
Scannez puis nettoyez et enfin redémarrez votre ordinateur.

2e étape : allez sur le site de https://ninite.com/
Cochez (1) Antivir **si** vous n'avez pas d'antivirus et (2) Malwarebytes, puis cliquez sur « get installer ».
Exécutez le fichier téléchargé.
L'installation est automatique, sans pub ni barre de navigation supplémentaire.

3e étape : lancez **Malwarebytes** et exécutez un scan complet.
À la fin du scan, cocher tout ce qui a été trouvé puis cliquez sur « supprimer la sélection » et c'est terminé !

4e étape : enfin, scannez votre ordinateur en ligne via :
https://www.eset.com/fr/home/products/online-scanner/