ANNEXE du Règlement Intérieur ENAC en vigueur

CHARTE INFORMATIQUE

L'ENAC met en œuvre un système d'information et de communication nécessaire à l'exercice de ses missions et de ses activités. Elle met à disposition de tous, des outils informatiques et de communication, c'est-à-dire des équipements informatiques en tout genre situés sur les sites de l'établissement qui sont dédiés à l'enseignements, à la recherche et à l'administration. Ces équipements sont de natures diverses et peuvent comprendre des postes de travail, des serveurs de données gérés par les administrateurs systèmes ou encore des équipements communs de réseau dont l'exploitation est assurée par les administrateurs réseaux de l'établissement. Cette charte définit ainsi les règles d'utilisation des moyens et équipements informatiques et des serveurs de l'ENAC tout en rappelant les droits et devoirs de chacun. Elle a pour objectif de sensibiliser les utilisateurs aux risques liées à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent avoir des conséquences graves de nature à engager sa responsabilité civile et/ou pénale ainsi que celle de l'établissement.

1. Domaine d'application

Ces règles s'appliquent à toute personne (dénommée dans ce texte " l'UTILISATEUR ") qui accède et qui utilise les moyens informatiques et de communication installés sur le site de l'ENAC : employés, élèves (étudiants), stagiaires, intérimaires, personnels de sociétés prestataires, personnels des clients de l'Ecole (ex : abonnés de la DFPV) visiteurs occasionnels, partenaires, collaborateurs, etc Ces moyens comprennent notamment les réseaux locaux et longue distance, les serveurs, les stations de travail, les micro-ordinateurs, les terminaux X et les autres périphériques. Dans ce qui suit, on désignera collectivement ces moyens sous le terme de 'SYSTEME INFORMATIQUE'. Les matériels de l'ENAC qui ne sont pas installés ou qui sont réformés, ainsi que les matériels mis à sa disposition, font par extension partie du SYSTEME INFORMATIQUE et leur utilisation est soumise aux même règles.

La gestion du SYSTEME INFORMATIQUE est assurée par des RESPONSABLES INFORMATIQUES désignés ; ils peuvent déléguer certaines de leurs tâches. Un ADMINISTRATEUR SYSTEME est un UTILISATEUR désigné par le RESPONSABLE INFORMATIQUE et disposant de droits et de devoirs spécifiques pour assurer l'administration d'une partie du SYSTEME INFORMATIQUE.

Ces règles s'appliquent aussi aux moyens informatiques auxquels il est possible d'accéder à

distance, directement ou en cascade, à partir du SYSTEME INFORMATIQUE, sans préjuger des règles applicables sur les sites distants.

2. Accès et utilisation du SYSTEME INFORMATIQUE

Les droits d'utilisation du SYSTEME INFORMATIQUE et d'accès, sont donnés par un RESPONSABLE INFORMATIQUE. Ils sont personnels et incessibles. Chaque utilisateur accède aux outils informatiques nécessaires à l'exercice de son activité professionnelle dans les conditions définies par l'ENAC. L'accès et l'utilisation du SYSTEME INFORMATIQUE sont limités aux activités de l'ENAC pour la bureautique, les cours, les études, recherches, stages et contrats. Ces droits disparaissent lorsque l'activité de l'utilisateur est terminée.

Lorsque l'utilisation d'un SYSTEME INFORMATIQUE implique l'ouverture d'un compte nominatif, l'UTILISATEUR s'en voit attribuer un par le RESPONSABLE INFORMATIQUE du site. Il protégera son compte par un mot de passe, qu'il s'engage à ne pas divulguer et qu'il choisira selon les règles de sécurité préconisées.

L'UTILISATEUR ne doit en aucun cas se servir d'un autre compte que celui qui lui a été attribué pour accéder au SYSTEME INFORMATIQUE. En cas d'utilisation d'un compte attribué à un groupe de personnes, l'utilisateur doit suivre la procédure définie à la création de ce compte par l'ADMINISTRATEUR SYSTEME et se conformer aux instructions données par l'ADMINISTRATEUR SYSTEME.

Tout utilisateur s'engage à respecter les règles de sécurité suivantes :

- Signaler au service informatique interne de l'ENAC toute violation ou tentative de violation suspectée de son compte intranet (ou réseau) et de manière générale tout dysfonctionnement
- Ne jamais demander son identifiant/mot de passer à un collègue ou à un collaborateur
- Ne pas masquer sa véritable identité
- Ne pas usurper l'identité d'autrui/d'un collègue
- Ne pas modifier les paramétrages du poste du travail à moins que cela soit nécessaire au bon fonctionnement du poste en question
- Ne pas installer des logiciels sans autorisation du service informatique
- Ne pas copier, modifier, détruire les logiciels propriétés de l'ENAC
- Verrouiller son ordinateur dès qu'il quitte son poste de travail
- Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas.

Toute copie de données sur un support externe est soumise à l'accord du supérieur hiérarchique et doit respecter les règles définies par l'ENAC

Les visiteurs ne peuvent avoir accès au SYSTEME INFORMATIQUE de l'ENAC sans l'accord préalable du service informatique interne. Par ailleurs, les intervenant extérieurs doivent s'engager à faire respecter la présente charte par leurs propres salariés et éventuelles entreprises sous-traitantes.

3. Respect de la législation

3.1 Le droit de la propriété intellectuelle

L'UTILISATEUR devra respecter les lois et les règlements en vigueur relatifs à la propriété intellectuelle des logiciels, et notamment le livre 1er du Code de la Propriété Intellectuelle. En particulier, il est rappelé :

- qu'il est strictement interdit à l'utilisateur d'effectuer des copies de logiciels commerciaux pour quelque usage que ce soit. Seules les copies de sauvegarde autorisées par la loi ou par la licence peuvent être faites. Il devra utiliser les logiciels conformément aux licences les concernant ;
- que la reproduction, la représentation ou la diffusion d'une œuvre de l'esprit ou d'une création protégée au titre de droits voisins est soumise au respect des droits de propriété intellectuelle et nécessite une cession et ou une autorisation émanant des titulaires des droits patrimoniaux et moraux prévus par le Code de la Propriété Intellectuelle sous peine de constituer le délit de contrefaçon de droit d'auteur

- que l'intrusion ou la tentative d'intrusion sur d'autres comptes ou d'autres systèmes informatiques sont des actions illicites.

que les signes distinctifs et inventions étant susceptibles de protection au titre des droits d propriété intellectuelle, leur reproduction, représentation ou diffusion est susceptible de constituer, à défaut de telles cessions et/ou autorisations, le délit de contrefaçon de marque ou de brevet

que les bases de données et les contenus en ligne sont protégés au bénéfice de leur auteur, outre par le droit d'auteur, par un droit spécifique sui generis (articles L.341-1 à L.343-1 du Code de la Propriété Intellectuelle)

Le signataire de la présente charte veillera à véhiculer et mettre à disposition sur le réseau local et Internet, seulement des données licites au regard des lois qui leur sont applicables. Il devra notamment respecter l'ensemble des dispositions légales applicables sur internet et en particulier le code de la propriété intellectuelle qui fait interdiction d'utiliser, de reproduire et plus généralement d'exploiter des œuvres protégées par le droit d'auteur sans l'autorisation de l'auteur ou des titulaires de droits.

3.2 Protection des données à caractère personnel

Si dans l'accomplissement de son travail/ ses activités, L'UTILISATEUR est amené à consulter ou à constituer des fichiers contenant des données à caractère personnel concernant des personnes physiques, il devra le faire en conformité avec la législation nationale et européenne en vigueur à savoir la loi Informatique et Liberté du 6 janvier 1978 modifiée et le Règlement UE/2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

En outre, L'UTILISATEUR est tenu de respecter l'ensemble du cadre légal lié à l'utilisation des systèmes d'information ainsi que toute autre réglementation susceptible de s'appliquer. En particulier, il doit respecter la loi du 29 juillet 1881 modifiée sur la liberté de la presse.

L'UTILISATEUR ne diffuse pas des informations constituant des atteintes à la personnalité (injures, discriminations, racisme, xénophobie, révisionnisme, diffamation, obscénité, pédopornographie, harcèlement ou menaces) ou pouvant constituer une incitation à la haine ou la violence ou une atteinte à l'image d'une personne, à ses convictions ou à sa sensibilité

la législation relative aux atteintes aux systèmes de traitement automatisé de données (articles L.323-1 et suivants du Code Pénal)

- La loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique
- les dispositions relatives au respect de la vie privée, de l'ordre public, du secret professionnel.

4. <u>Droits et devoirs des UTILISATEURS</u>

4.1 Accès et confidentialité

L'accès aux informations conservées sur le SYSTEME INFORMATIQUE doit être limité aux fichiers personnels de l'UTILISATEUR, aux fichiers communs à un groupe d'utilisateurs auquel il appartient et aux fichiers publics. En particulier, il est interdit de copier ou de prendre connaissance d'informations détenues par d'autres UTILISATEURS, sans leur autorisation, quand bien même ceux-ci ne les auraient pas explicitement protégées. Cette règle s'applique également aux échanges privés, du type messagerie électronique ou conversation directe, dont l'UTILISATEUR n'est destinataire ni directement, ni en copie.

L'UTILISATEUR fait preuve de vigilance vis-à-vis des informations reçues (désinformation, virus informatique, tentative d'escroqueries, chaînes, hameçonnage, etc.). En présence de d'un doute vis-à-vis d'une information reçue, il doit contacter le service informatique.

Lors de son départ, l'UTILISATEUR doit restituer au service informatique interne les matériels qui ont été mis à sa disposition durant ses activités. Il doit préalablement effacer ses fichiers personnels et ses données privées du ou des postes de travail utilisé(s). Toute copie de tout document professionnel est strictement interdite à moins qu'il y ait une autorisation de la part du chef de service. Les comptes et les données personnelles de l'UTILISATEUR sont, en tout état de cause, supprimés dans un délai maximum (A COMPLETER) après son départ.

4.2 Intégrité des informations

L'UTILISATEUR s'engage à ne pas modifier ou détruire d'autres fichiers que ceux qui lui appartiennent en propre, sauf accord de leur propriétaire. En particulier, il lui est interdit de modifier le ou les fichiers contenant des informations comptables ou d'identification.

4.3 Intégrité des systèmes informatiques

L'UTILISATEUR s'engage à ne pas apporter volontairement des perturbations du système informatique, soit par des manipulations anormales du matériel, soit par des modifications de logiciel, soit par l'introduction de logiciels parasites connus sous le nom générique de virus, soit par tout autre moyen.

La connexion de nouvelles machines, la modification de la connexion de machines existantes, de sous- réseaux, l'ajout de type d'équipement ou de services réseaux gérés par l'ENAC ne pourront être faits que par le Pôle des Système d'Information.

L'installation de nouveaux logiciels ou la modification de logiciels existants, ayant un impact sur des programmes ou des bibliothèques utilisées par la communauté des usagers ne pourront être faits que par le Pôle des système d'information.

4.4 Abus de ressources et déontologie

L'UTILISATEUR ne doit pas oublier qu'il vit et travaille au sein d'une communauté. Il s'interdit toute utilisation abusive d'une ressource commune (imprimante, réseau, espace disque, processeur…). Il s'interdit également de perturber tout autre utilisateur du SYSTEME INFORMATIQUE à l'aide d'outils électroniques, de masquer sa véritable identité ou de s'approprier le mot de passe d'un autre utilisateur.

Il s'interdit également de porter atteinte à l'intégrité ou à la sensibilité d'un autre utilisateur, notamment par l'intermédiaire de messages ou d'images provocants. La messagerie mise à

disposition des utilisateurs est uniquement destinée à un usage professionnel. Néanmoins, tout message qui comportera la mention expresse ou manifeste de son caractère personnel, bénéficiera du droit au respect de la vie privée et du secret des correspondances. A défaut, le message est présumé professionnel.

Il s'interdit également à travers les messages envoyés à l'adresse de messagerie ENAC Globale, de mettre en cause ou de porter préjudice, à un ou des collègues au sein de l'ENAC.

Il s'interdit enfin de saturer la messagerie des autres utilisateurs par l'envoi de messages, soit trop nombreux, soit trop volumineux (taille des pièces jointes), non liés à son activité professionnelle.

Les employés peuvent consulter leur messagerie professionnelle à distance à l'aide d'un navigateur (webmail). Les fichiers qui seraient copiés sur l'ordinateur personnel utilisé par l'employé dans ce cadre doivent être effacés dès que possible dudit ordinateur sous peine de sanctions.

L'accès au réseau Internet est exclusivement réservé à un usage professionnel conforme à la finalité du fournisseur d'accès Internet de l'ENAC (recherche, enseignement, développements techniques et transfert de technologies, diffusion d'informations scientifiques, techniques et culturelles). Ainsi, les utilisateurs peuvent consulter les sites Internet souhaités tout en présentant un lien direct et nécessaire avec l'activité professionnelle ou pédagogique.

L'utilisateur s'engage à une utilisation loyale des ressources du réseau local et du réseau Internet en prévenant et s'abstenant de toute utilisation malveillante destinée à perturber ou porter atteinte aux réseaux.

4.5 Responsabilité de l'UTILISATEUR

En cas de de manquement aux présentes règles et mesures de sécurité définies par la présente charte ou de violation de la clause de confidentialité, par l'UTILISATEUR autorisé, celui-ci est susceptible d'engager sa responsabilité civile et pénale sur les conséquences de ses actes et peut en outre faire l'objet de sanctions disciplinaires. Le non-respect des lois et textes applicables en matière de sécurité des systèmes d'information est susceptible de sanctions pénales. L'ENAC se réserve le droit de lui interdire l'accès au SYSTEME INFORMATIQUE sans préavis et de prendre toutes les mesures qu'il jugera nécessaires.

4.6 Droits et devoirs des administrateurs systèmes

A des fins de maintenance informatique, le service informatique interne de l'ENAC peut accéder à

distance à l'ensemble des postes de travail. Cette intervention s'effectue avec l'autorisation expresse de l'utilisateur. Les administrateurs systèmes peuvent examiner modifier ou détruire certains fichiers pour l'application des règles de sécurité, ou dans le cadre de leur travail de configuration générale (exemple : interdiction des fichiers .rhosts, mot de passe dans les fichiers, etc.) Cependant, les fichiers utilisateurs ne peuvent être modifiés, détruits ou restaurés qu'après accord de leur propriétaire.

Les administrateurs systèmes sont liés par le secret professionnel. Ils s'interdisent de lire le contenu des messages ou des fichiers qui ne leur sont pas destinés et dont ils pourraient avoir connaissance par leur fonction ou leurs droits d'accès.

Pour assurer la sécurité du système informatique, contrôler le respect des règles définies par la présente charte et pour disposer de données statistiques et comptables, l'administrateur a accès aux fichiers de trace de l'activité des utilisateurs dont notamment les fichiers suivants : fichier log de la messagerie, fichier log du " proxy " http, fichier log du " proxy " FTP, fichier de configuration et d'accès aux news. Ces traces sont exploitées par des outils de surveillance. L'administrateur système doit assurer la confidentialité de ces traces, mais peut les utiliser pour mettre en évidence certaines infractions.

4.7 Les traitements informatiques permettant de tracer l'activité des utilisateurs

Les traitements informatiques des données permettant de tracer l'activité des utilisateurs effectuée grâce/avec le SYSTEME INFORMATIQUE doivent respecter la législation en vigueur en la matière :

- La loi Informatique et Libertés du 6 janvier 1978 modifiée
- Le Règlement UE/2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

Les utilisateurs disposent de plusieurs droits concernant ces traitements qu'ils peuvent exercer auprès du Délégué à la Protection des Données désigné au sein de l'établissement.

Je soussigné(e) : ……..

certifie avoir pris connaissance des règles de bonne conduite énoncées dans le présent document et m'engage à m'y conformer strictement.

A *le*

(signature à faire précéder de la mention manuscrite " lu et approuvé ")

ANNEX of ENAC Internal rules

INFORMATION TECHNOLOGY CHARTER

The ENAC implements an information and communication system necessary for carrying out its missions and its activities. It makes IT and communication tools available to everyone, i.e. computer equipment of all kinds located on the sites of the School which are dedicated to teaching, research and administration. This equipment is of various kinds and may include workstations, data servers managed by system administrators or common network equipment whose operation is ensured by the school's network administrators. This Charter sets out the rules for the use of ENAC's computer resources and equipment and servers while recalling the rights and duties of each person. Its purpose is to raise awareness among users of the risks related to the use of these resources in terms of integrity and confidentiality of the information processed. These risks require that certain security and good conduct rules are respected. Carelessness, negligence or malice of a user may have serious consequences and thereby involve their civil and/or criminal liability as well as that of the School.

1. Scope

These rules apply to any person (referred to in this text as the "USER") who accesses and uses the computer and communication resources installed on the ENAC site: employees, students, trainees, temps, the staff of service provider companies, staff of customers of the School (e.g. subscribers to the DFPV) occasional visitors, partners, collaborators, etc. These resources include, in particular, the local and long distance networks, servers, workstations, micro-computers, X terminals and other devices. In what follows, these resources will be collectively called the 'IT SYSTEM'. ENAC equipment which is not installed or which has been withdrawn, as well as the equipment placed at its disposal, by extension form part of the IT SYSTEM and their use is subject to the same rules.

Management of the IT SYSTEM is provided by appointed IT MANAGERS; they may delegate some of their tasks. A SYSTEM ADMINISTRATOR is a USER appointed by the IT MANAGER who has specific rights and duties to administer part of the IT SYSTEM.

These rules also apply to the computer resources which it is possible to access remotely, directly or indirectly, from the IT SYSTEM, without prejudice to the rules applicable on remote sites.

2. Access and use of the IT SYSTEM

The rights of use of the IT SYSTEM and access to it, are given by an IT MANAGER. They are personal and non-transferable. Each user accesses the tools necessary for carrying out their work under the conditions laid down by ENAC. Access to and use of the IT SYSTEM are limited to ENAC's activities for office automation, courses, studies, research, internships and contracts. These rights disappear when the user's activity is completed.

When using an IT SYSTEM involves opening a named account, the USER is assigned one by the

site's IT MANAGER. They must protect their account with a password, that they undertakes not to disclose and that they must choose in accordance with the recommended security rules.

The USER must in no case use an account other than the one that has been assigned to them to access the IT SYSTEM. If an account is assigned to a group of people, the user must follow the procedure defined when the SYSTEM ADMINISTRATOR created the account and comply with the instructions given by the SYSTEM ADMINISTRATOR.

Any user undertakes to comply with the following security rules:

- Report to the ENAC's internal IT department any violation or suspected attempted violation of their intranet account (or network) and, generally, any malfunction
- Never ask a colleague or a member of staff for their login/password
- Not hide their true user identity
- Not steal the user identity of another person/a colleague
- Not change the workstation settings unless necessary for the proper operation of the station in question
- Not install software without permission from the IT department
- Not copy, modify, destroy software belonging to ENAC
- Lock the computer as soon as they leaves their workstation
- Not access, attempt to access, delete or modify information that does not belong to them

Agreement of the supervisor must be obtained for any copy of data onto an external medium and this must comply with the rules set out by ENAC
Visitors may not have access to the ENAC's IT SYSTEM without the prior agreement of the internal IT department. Moreover, external actors must undertake to ensure this Charter is complied with by their own employees and any sub-contractors.

3. Compliance with the legislation

3.1 Intellectual property rights

The USER must comply with the laws and regulations in force relating to the intellectual property of software, and in particular, Book 1 of the Intellectual Property Code. In particular, it is recalled:

- that the user is strictly forbidden from making copies of commercial software for any purpose whatsoever. Only the backup copies permitted by law or by the licence can be made. They must use the software in accordance with the relevant licences;
- that the reproduction, representation or dissemination of a work of the mind or a creation protected under neighbouring rights is subject to compliance with intellectual property rights and requires an assignment and permission from the holders of the economic and moral rights provided for by the Intellectual Property Code, failing which the latter constitutes the offence of copyright infringement

- that the intrusion or the attempted intrusion into other accounts or other IT systems are unlawful actions.

that since distinctive signs and inventions may be protected by intellectual property rights, their reproduction, representation or dissemination may constitute, in the absence of such assignments and/or permissions, the offence of trademark or patent infringement

that databases and online content are protected in favour of their author, in addition to copyright, by a specific sui generis law (Articles L.341-1 to L.343-1 of the Intellectual Property Code)

The signatory of this Charter must take care to transmit and make available on the local network and on the Internet, only data that is lawful under the laws that are applicable to them. They must in particular comply with all the applicable legal provisions on the Internet and in particular the Intellectual Property Code which prohibits the use, reproduction and more generally the exploitation of works protected by copyright without the permission of the author or holders of the rights.

3.2 Protection of personal data

If when carrying out their work/activities, the USER views or constitutes files containing personal data relating to natural persons, they must do so in compliance with the national and European legislation in force namely the amended Computing and Freedom Act of 6 January 1978 and EU Regulation/2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

In addition, the USER must comply with the entire legal framework related to the use of information systems as well as any other regulation that may apply. In particular, they must comply with the amended Act of 29 July 1881 on the freedom of the press.

The USER may not disseminate information constituting violations of a person's rights (insults, discrimination, racism, xenophobia, revisionism, defamation, obscenity, child pornography, harassment or threats) or that may constitute an incitement to hatred or violence or an attack on a person's image, beliefs or sensitivity

the legislation relating to violations of automated data processing systems (Articles L.323-1 and following of the Criminal Code)

- Act No. 2004-575 of 21 June 2004 for trust in the digital economy
- the provisions relating to respect of privacy, public order, professional secrecy.

4. <u>USERS' rights and duties</u>

4.1 Access and non-disclosure

Access to the information stored on the IT SYSTEM must be limited to the USER's personal files, to the files common to a group of users to which they belong and to public files. In particular, it is forbidden to copy or become aware of information held by other USERS, without their permission, even when the latter have not explicitly protected it. This rule also applies to private communications, such as email or direct conversations, of which the USER is not the addressee, either directly or copied in.

The USER must be vigilant with regard to the information received (misinformation, computer virus, scam attempts, chains, phishing, etc.). If in doubt regarding an item of information received, they must contact the IT department.

When they leave, the USER must return to the internal IT department the materials which have been placed at their disposal during their activities. They must first erase their personal files and their private data from the workstation(s) used. Any copy of any professional document is strictly prohibited unless permitted by the head of department. The USER's accounts and personal data are, in any event, deleted within a maximum period of (TO BE COMPLETED) after their departure.

4.2 Integrity of the information

The USER undertakes not to modify or destroy files other than those which personally belong to them, except with their owner's agreement. In particular, they may not change the file or files containing accounting or identification information.

4.3 Integrity of the IT systems

The USER undertakes not to intentionally disrupt the IT system, either through abnormal handling of the equipment, or by software changes, or by introducing software parasites known under the generic name of viruses, or by any other means.

The connection of new machines, changing the connection of existing machines, sub-networks, the addition of equipment or network services managed by ENAC may be made only by the Information System Centre.

The installation of new software or the modification of existing software having an impact on the programs or libraries used by the community of users may be made only by the Information System Centre.

4.4 Misuse of resources and ethics

The USER must not forget that they live and work in a community. They must not misuse a common resource (printer, network, disk space, processor, etc.). They must also refrain from disrupting any other user of the IT SYSTEM using electronic tools, from hiding their true identity or appropriating another user's password.

They must refrain from violating the integrity or sensitivity of another user, in particular through provocative messages or images. The email system made available to users is intended for professional use only. Nevertheless, any message which includes the express or clear indication of its personal nature, will benefit from the right to respect for privacy and the secrecy of correspondence. By default, the message is presumed to be professional.

They must also refrain, through messages sent to the ENAC Globale email address from undermining or causing damage to one or more colleagues within ENAC.

Finally, they must refrain from saturating the email system of other users by sending messages that are either too many or too large (size of attachments), unrelated to their work.

Employees may view their professional email remotely using a browser (webmail). Any files copied onto a personal computer used by the employee in this context must be deleted as soon as possible from the said computer or risk penalties.

Access to the Internet is reserved exclusively for professional use consistent with the purpose of the Internet service provider of the ENAC (research, teaching, technical developments and technology transfer, dissemination of scientific, technical and cultural information). Thus, users may visit the websites they wish to provided they have a direct and necessary link with the professional or educational activity.

The user undertakes to make fair use of the resources of the local network and the Internet by averting and refraining from any malicious use intended to disrupt or harm the networks.

4.5 The USER’s liability

In the case of a violation of these rules and the security measures set out in this Charter or a violation of the non-disclosure clause, by the authorised USER, the latter’s civil and criminal liability may be sought for the consequences of their actions and in addition they may be subject to disciplinary penalties. Non-compliance with the laws and texts applicable regarding the security of the information systems exposes the person concerned to criminal penalties. ENAC reserves the right to deny them access to the IT SYSTEM without notice and to take all the measures that it deems necessary.

4.6 Rights and duties of systems administrators

In order to perform computer maintenance, the internal IT department of ENAC may remotely access all the workstations. This operation is carried out with the user's express permission. System administrators may examine, modify or destroy some files for the application of the security rules, or as part of their general configuration work (e.g. prohibition of .rhosts files, password in files, etc.) However, the users’ files may only be modified, destroyed or restored after agreement from their owner has been obtained.

System administrators are bound by the professional secrecy obligation. They are prohibited from reading the content of messages or files that are not intended for them and about which they could have knowledge due to their position or their access rights.

To ensure security of the IT system, check compliance with the rules set out in this Charter and to have statistical and accounting data, the administrator has access to the log files of the users' activity including in particular the following files: email log file, "proxy" http log file, "proxy" FTP log file, configuration file and access to the news. These logs are used by monitoring tools. The system administrator must ensure the confidentiality of these logs, but may use them to reveal certain offences.

4.7 Computer processing tracking users' activity

Computer processing of data used to track the activity of users carried out thanks to/with the IT SYSTEM must comply with the legislation in force in this regard:

- The amended Computer and Freedoms Act of 6 January 1978
- EU Regulation/2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Users have several rights regarding this processing that they can exercise by contacting the Data Protection Officer in the school.

I, the undersigned: .....

certify having acquainted myself with the good behaviour rules stated in this document and commit myself to strictly conform with them.

..... , ...

(signature preceded by the handwritten mention "read and approved")