ÉCOLE FRANÇAISE
DE ROME

Charte d'usage du système d’information de l'École française de Rome

Sommaire

Préambule

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.

Le "système d'information" recouvre l'ensemble 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 du réseau de l'École française de Rome.

L'informatique nomade (assistants personnels, les ordinateurs portables, les téléphones portables, etc.), est également un des éléments constitutifs du système d'information.

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.

Le terme "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.

Le terme "établissement" désigne l' "École française de Rome"

Les personnels du service informatique en charge 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 identifiées comme telles ; elles relèvent de la vie privée de l'utilisateur ;
- elles ne mettent pas en cause le bon fonctionnement du système d'information et sa sécurité ;
- elles ne tombent pas dans le champ du non-respect de la législation applicable.

Engagements de l'établissement

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

L'établissement, par l'intermédiaire du service informatique, met en œuvre les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisateurs.

L'établissement permet 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[1].

L'utilisateur s'engage à respecter scrupuleusement les règles indiquées par le service informatique sur l'utilisation, l'accès, et les consignes de sécurité liées au système d'information.

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] 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 utilisateurs accédant au système d'information sont :

- tout personnel, titulaire ou non titulaire de l'École française de Rome; concourant à l'exécution des missions de l'établissement ;
- toute personne extérieure à l'établissement, visiteur, invité, prestataire[2], ayant contracté avec l'établissement.

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 un mois après que celui-ci n'a 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 en général. Pour les données sensibles (pour lesquelles a été identifié un besoin direct ou indirect de confidentialité), il doit notamment éviter de les communiquer ou de 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.

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, de formation, de documentation, de valorisation et d'administration. 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…) utilisé.

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 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.

---

[2] Toute forme de contrat doit prévoir expressément l'obligation de respect de la charte.
[3] Pour exemple, cet espace pourrait être dénommé « _privé_ »
[4] Pour exemple, « _privé_nom_de_l_objet_ » : l'objet pouvant être un message, un fichier ou tout autre ressource numérique.

Les mesures de conservation des données professionnelles sont définies par le service informatique de l'établissement.

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

Article V. Principes de sécurité

Section V.1 Règles de sécurité applicables

Le service informatique 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 qu'il reçoit 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.

L'utilisateur ne peut pas enregistrer les codes d'accès sur des supports électroniques internes ou externes à l'établissement (ordinateur, téléphone, tablette…) même si des fonctionnalités du matériel informatique le permettent.

L'utilisateur s'engage à ne pas confier à des systèmes externes les codes d'accès.

Les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est confiérée. 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 ses codes d'accès et ne pas les 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 verrouiller sa session lorsqu'il quitte son poste de travail.

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 ;
- limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité.

✓ 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 ;
- s'interdire d'accéder ou de tenter d'accéder à des ressources externes au système d'information de l'établissement, pour lesquelles il n'a pas reçu d'habilitation explicite ;
- ne pas connecter directement aux réseaux locaux de l'établissement des matériels autres que ceux autorisés par le service informatique ;
- ne pas installer, télécharger ou utiliser sur le matériel de l'établissement, des logiciels ou progiciels autres que ceux autorisés par le service informatique ;
- ne pas utiliser un ordinateur privé sur le réseau sans fil qui ne soit doté d'un antivirus, actif, efficace et à jour, l'ordinateur ne doit pas être doté de logiciels malveillants (analyse de réseau, partages de bandes …) ;
- ne pas modifier ou faire modifier par un tiers le matériel et les logiciels mis à disposition par le service informatique ;
- respecter le droit à la propriété intellectuelle ;
- se conformer aux dispositifs mis en place par le service informatique pour lutter et prévenir les attaques (virus, programmes informatiques malveillants …) ;
- 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.

Section V.2 Devoirs de signalement et d'information

L'utilisateur doit avertir le service informatique sans délai de tout dysfonctionnement ou de toute anomalie constatée. 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 :

- qu'il doit sans délai autoriser et permettre au service informatique d'intervenir pour effectuer la maintenance corrective, curative ou évolutive ; le service informatique se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition ;
- que toute information bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire sera isolée et si nécessaire supprimée ;
- que tout matériel compromis ou résultant comme un possible péril pour le système d'information peut être neutralisé sans délai et sans préavis par le service informatique ;
- 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.

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, si celui-ci est rattaché à l'établissement, 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'utilisateur communique avec cette adresse électronique pour toutes les actions internes ou externes concourant à l'exécution des missions de l'établissement.

L'utilisateur s'engage à ne pas donner à des systèmes externes les codes d'accès et l'utilisation de sa boîte à lettres.

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[5] 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 du Règlement Général sur la Protection des Données (RGPD).

La transmission de données sensibles[6] est interdite sauf par dispositif spécifique chiffré agréé par le service informatique.

(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…).

---

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

[6] Il s'agit de la protection des données selon le RGPD

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.

L'utilisateur doit s'assurer de respecter le RGPD avant d'envoyer des messages aux destinataires, notamment pour éviter que l'établissement soit classifié comme émetteur de pourriels dont la conséquence très pénalisante est le blocage des courriels.

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 doit être validée par un responsable de site ou responsable de publication nommément désigné.

(b) Sécurité

Pour préserver la sécurité du système d'information de l'établissement, le service informatique 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, d'intervenir et de modifier le système d'information de l'établissement.

Les accès ne sont autorisés qu'au travers des dispositifs de sécurité mis en place par le service informatique et des règles de sécurité spécifiques peuvent être précisées par le service informatique.

L'utilisateur est informé des risques et limites inhérents à l'utilisation d'Internet par le biais d'actions de formation obligatoires à suivre 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.

Le service informatique 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

Le service informatique se réserve le droit de mettre en place des outils de traçabilité et journalisation sur tous les systèmes d'information.

Article VIII. Respect de la propriété intellectuelle

L'établissement rappelle que l'utilisation des ressources informatiques 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 écrite des titulaires de ces droits en respectant le modèle fourni par l'établissement.

Article IX. 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, il doit mettre en œuvre le RGPD (protection des données).

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 autorisation écrite par le délégué à la protection des données (DPO) de l'établissement.

Article X. Télétravail

L'usage du télétravail implique pour l'utilisateur la nécessité de respecter l'ensemble des articles de cette charte.

Le télétravail s'effectue avec un matériel informatique de l'établissement, configuré par le service informatique et remis à l'utilisateur, ou bien par un matériel informatique de l'utilisateur dument validé par le service informatique et au besoin configuré par le service informatique, afin d'accéder à distance au système d'information de l'établissement et permettre à l'utilisateur d'effectuer ses missions.

La remise du matériel informatique de l'établissement à l'utilisateur fait l'objet d'un bon de livraison signé par l'utilisateur.

Si l'utilisateur utilise une connexion sans fil (wifi), la connexion doit utiliser le cryptage de niveau maximum, en aucun cas le réseau ne doit être ouvert.

Sur demande du service informatique, le matériel mis à disposition par l'établissement est ramené dans les meilleurs délais au service informatique.

Article XI. Limitation des usages

En cas de non-respect des règles définies dans la présente charte et des modalités d'utilisations définies par le service informatique, l'utilisateur pourra être limité dans l'usage du système d'information de l'établissement par mesure conservatoire.

En cas de compromission d'un élément interne ou externe au système d'information de l'établissement, le service informatique pourra interdire son usage.

Article XII. Entrée en vigueur de la charte

La charte informatique entrera en vigueur à la date du 17 septembre 2020.

Elle est annexée au règlement intérieur et sera mise à jour autant que de besoin.