École nationale des chartes

PSL

CHARTE D'UTILISATION DES RESSOURCES INFORMATIQUES

TITRE I – OBJET ET CHAMP D'APPLICATION

ARTICLE 1 – Objet

La présente charte définit les droits et obligations des utilisateurs du Système d'Information (SI) et des Technologies de l'Information et de la Communication (TIC) mis à disposition par l'Ecole nationale des chartes. Elle intègre et décline les dispositions légales et réglementaires qui s'imposent à l'établissement et aux utilisateurs et utilisatrices.

Elle est complétée par des annexes, notamment par :
- Annexe A – Restrictions d'utilisation d'internet ;
- Annexe B – Politique de confidentialité des données des personnels ;
- Annexe C – Politique de confidentialité des données des étudiants ;
- Annexe D – Registre des activités de traitement ;
- Annexe E – Décision de nomination du DPO ;
- Annexe F – Charte informatique de l'Université PSL.

ARTICLE 2 - Domaine d'application

1. Utilisateurs et utilisatrices

On désigne sous le terme « utilisateur » et « utilisatrice » toute personne physique ou morale, sans exception, disposant d'un accès, utilisant ou intervenant sur les ressources du système d'Information mis à disposition par l'École nationale des chartes.
Les règles et procédures prévues dans la présente charte s'imposent à tout utilisateur et utilisatrice quel que soit son statut (personnels, stagiaires, enseignants, élèves, étudiants, vacataires, chercheurs, prestataires externes intervenant en sous-traitance, usagers, personnes invitées, sans que cette liste ne soit exhaustive) ou sa situation géographique vis-à-vis de l'École nationale des chartes.

2. Ressources

On entend par Système d'Information (SI) et Technologies de l'Information et de la Communication (TIC) l'ensemble des moyens matériels, des logiciels, des bases de données et des réseaux de communication pouvant être mis à disposition des utilisateurs et des utilisatrices.
L'accès à cet ensemble à distance, par un poste fixe ou par l'informatique « nomade » (assistants personnels, ordinateurs portables, smartphones etc.), relève également de la présente charte. Il en est de même de toute nouvelle

technologie de l'information et de communication mise à disposition par l'Ecole nationale des chartes.

TITRE II – UTILISATION ET BON USAGE DES SYSTEMES

ARTICLE 3 - Règles d'utilisation du matériel

L'utilisation des ressources du système d'information et l'usage des services Internet sont autorisés dans le cadre de l'activité professionnelle, scolaire, d'enseignement, de recherche et présumés l'être à cette fin. L'utilisation de tels systèmes peut être le cas échéant pour des besoins personnels à la condition que cet usage présente un caractère limité en nombre et en durée de connexions et qu'il ne porte pas atteinte aux usages autorisés.

L'accès aux réseaux et aux différents systèmes informatiques est strictement personnel et ne peut en aucun cas être cédé, même temporairement, à un tiers. Il peut être retiré à tout moment. Toute autorisation prend fin lors de la cessation de l'activité professionnelle, scolaire, d'enseignement et de recherche pour laquelle elle a été initialement concédée.

Tout utilisateur ou utilisatrice est responsable de l'usage qu'il fait des ressources du système information auxquelles il a accès. L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation ou leur détournement à des fins personnelles.

L'utilisateur ou l'utilisatrice a la charge, à son niveau, de contribuer à la sécurité générale du système d'information de l'Ecole nationale des chartes. Il ou elle doit notamment appliquer les recommandations de sécurité de l'Ecole nationale des chartes mentionnées à l'article 11 de la présente charte, assurer la protection de ses informations en utilisant les différents moyens de sécurité mis à sa disposition, en choisissant notamment des mots de passe sûrs et gardés secrets et être responsable du bon usage de ses droits.

En outre, l'utilisateur ou l'utilisatrice se doit de signaler toute anomalie qu'il ou elle peut constater au Responsable de la Sécurité des Systèmes d'Information (RSSI) de l'Ecole nationale des chartes. Il doit veiller à ne pas installer de logiciels, ni contourner ses restrictions d'utilisation. En dehors d'autorisations exceptionnelles et spécifiques, seules les équipes du Centre de ressources informatiques sont autorisées à installer les logiciels dûment acquis par l'École nationale des chartes.

Afin d'éviter tout usurpation d'identité, l'utilisateur ou l'utilisatrice doit veiller à ne pas laisser son matériel sans surveillance et sans se déconnecter (session, comptes...) en laissant des ressources ou services accessibles. Il ou elle doit également veiller à ne pas utiliser ou essayer d'utiliser des droits autres que les siens, de masquer sa véritable identité ou d'usurper celle

d'autrui.

ARTICLE 4 – Règles d'utilisation des services internet et messagerie

Il appartient à l'utilisateur ou à l'utilisatrice de procéder au stockage éventuel de ses fichiers à caractère privé dans un espace prévu explicitement à cet effet (espace exclusivement dénommé « privé » ou « personnel ») dont la responsabilité et la sauvegarde lui incombent. Cet espace est à localiser sur les disques durs du poste informatique et autres périphériques de l'utilisateur ou de l'utilisatrice et en aucun cas sur les serveurs de fichiers (lecteurs réseaux nominatifs ou communs) ou sur un espace virtuel de stockage mis à sa disposition par l'École nationale des chartes. Il lui revient également d'identifier explicitement ses courriels à caractère strictement privé, en ajoutant « personnel » ou « privé » dans l'objet.

Afin d'assurer la continuité de service, l'utilisateur ou l'utilisatrice doit privilégier le dépôt de ses fichiers de travail sur des zones partagées par les membres de son service ou de son équipe.

En cas de départ, ou d'absence prolongée, l'utilisateur ou l'utilisatrice informe l'École nationale des chartes des modalités permettant l'accès aux ressources mises spécifiquement à sa disposition. En tout état de cause les données non situées dans un espace identifié comme privé, sont considérées comme appartenant à l'École nationale des chartes qui pourra en disposer. En particulier, l'École nationale des chartes se réserve le droit d'accéder aux messageries professionnelles dans certaines circonstances telles que les besoins liés à l'organisation du travail, la préservation des preuves en cas de litige ou le respect des obligations légales.

L'utilisateur ou l'utilisatrice doit veiller à ne pas se connecter ou essayer de se connecter sur un serveur, interne ou externe, autrement que par les dispositions prévues par la Politique de Sécurité des Systèmes d'Information (PSSI) de l'École nationales des chartes ou sans y être autorisé. Il ou elle ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il ou elle accède. L'usage des ressources qui sont confiées à l'utilisateur ou l'utilisatrice ne doit pas être contraire à la réglementation en vigueur (ex : téléchargement illégal d'œuvres de l'esprit, visionnage illégal de programmes audiovisuels en « streaming »).

Enfin, il ou elle doit veiller à ne pas utiliser ces ressources pour proposer ou rendre accessibles aux tiers des données et informations confidentielles ou contraires à la législation en vigueur.

L'utilisateur ou l'utilisatrice doit faire preuve de la plus grande correction et discrétion à l'égard de ses interlocuteurs ou interlocutrices dans les échanges et notamment pour les courriers, forums de discussions, intranet, etc. A cet

égard, il ou elle doit notamment veiller à ne pas émettre d'opinions susceptibles de porter préjudice à l'École nationale des chartes.

L'École nationale des chartes ne peut être tenue pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se conforme pas à ces règles.

L'accès au service de messagerie a vocation à être fermé dès que l'utilisateur ou l'utilisatrice quitte les effectifs de l'établissement. Pour les agents administratifs, l'accès sera fermé le jour suivant leur départ. Pour les enseignants-chercheurs titulaires, l'accès sera maintenu pendant 1 an après le départ de l'établissement et, pour les enseignants-chercheurs non titulaires (contrats docs, post-docs, ATER), pendant 3 mois. Pour les élèves ou étudiants, l'accès sera maintenu pendant deux ans après l'obtention du diplôme.

Préalablement à la clôture de l'accès à la messagerie dans les cas cités ci-dessus, l'utilisateur ou l'utilisatrice est invité(e) à faire le tri de ses messages préalablement à son départ, notamment à supprimer toutes données personnelles. Un message type l'en informe dès que l'établissement a connaissance de son départ prochain.

La boîte de messagerie en elle-même restera consultable par l'administration pendant 1 an après la fermeture de l'accès, afin de pouvoir effectuerl'archivage nécessaire.

Les usages relevant de l'activité des organisations syndicales et de leurs représentants sont régis par les dispositions législatives et règlementaires en vigueur. Dans ce cadre, les listes de diffusion syndicales ainsi que les pages syndicales ouvertes sur le site de type intranet ou de réseau social interne sont libres d'expression, des restrictions ne pouvant intervenir que conformément à la législation en vigueur.

Les listes de diffusion à destination des élèves, des étudiants et étudiantes ou des enseignants et enseignantes sont réservées à l'équipe de direction et de la scolarité de l'École nationale des chartes. Elles sont utilisées pour communiquer des informations liées à la scolarité et à la pédagogie. Leur usage par tout autre utilisateur et/ou à toute autre fin, devra avoir fait l'objet d'une autorisation préalable de l'administration de l'École nationale des chartes.

ARTICLE 5 - Confidentialité et protection des libertés individuelles

L'accès par l'utilisateur ou l'utilisatrice aux informations et documents conservés sur les systèmes d'information doit être limité à ceux qui lui sont propres, et ceux qui sont publics ou partagés.

Il est strictement interdit de prendre connaissance d'informations détenues par d'autres utilisateurs ou utilisatrices soit sur leur messagerie soit sur leur session qui leur sont personnelles, quand bien même ceux-ci ne les auraient pas explicitement protégées.

Il pourra être dérogé à cette règle pour des motifs impérieux de bon fonctionnement des services et notamment afin d'assurer leur bonne continuité ou encore la sécurité des systèmes d'information ainsi que pour tout autre cas autorisé par les dispositions législatives et réglementaires en vigueur. La décision devra être prise par l'employeur ou son représentant dans le cas des personnels, et du chef d'établissement ou de son délégataire dans le cas des élèves, étudiants et étudiantes et enseignants et enseignantes.

L'utilisateur ou l'utilisatrice, s'interdit de noter dans le système d'information des informations prohibées relatives à la vie privée des tiers, collaborateurs et collaboratrices, élèves, étudiants et étudiantes, enseignants et enseignantes, ainsi que d'émettre des opinions pouvant avoir un caractère injurieux, raciste, pornographique ou diffamatoire.

ARTICLE 6 - Respect du droit de propriété intellectuelle et de la vie privée

Les utilisateurs et les utilisatrices doivent respecter les dispositions du code de la propriété intellectuelle.

A ce titre, ils doivent notamment utiliser les logiciels dans les conditions des licences souscrites. Il est strictement interdit de 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 sans avoir obtenu l'autorisation du ou des titulaire(s) des droits (les logiciels et documents « libres » relèvent aussi de ces dispositions).

De la même façon, les marques ne peuvent être utilisées sans autorisation du ou des propriétaire(s).

L'auteur d'une contrefaçon engage directement sa responsabilité, il peut être poursuivi devant les tribunaux ainsi que le cas échéant, la personne morale qui l'emploie.

Aucune captation (cours, réunions, forum...sans que cette liste ne soit exhaustive) ne doit porter atteinte à l'intégrité, la dignité ou à l'image des personnes concernées, et ne peut être utilisée à une fin autre que celle à laquelle les participants ont librement consenti. Toute utilisation commerciale non autorisée au préalable est proscrite.

Dans le cadre des enseignements à distance, les cours enregistrés pourront être utilisés à des fins pédagogiques dans le seul but d'être visionnés et

revisionnés par les élèves, étudiants et étudiantes régulièrement inscrits.

Conformément aux articles 226-1, 226-2 et 226-8 du code pénal, toute personne qui contreviendrait aux dispositions qui précèdent s'expose à des sanctions pénales si elle diffuse, partage, ou communique par n'importe quel moyen, ces images, animées ou non, et/ou les paroles en dehors de ce cadre universitaire.

ARTICLE 7 - Préservation de l'intégrité

L'utilisateur ou l'utilisatrice s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes d'information et des réseaux notamment par des manipulations anormales du matériel ou par l'introduction de logiciels malveillants.

L'implantation, l'utilisation, le développement ou la diffusion de programmes mettant en cause l'intégrité des systèmes sont prohibés. Il est interdit de se livrer depuis des systèmes appartenant à l'École nationale des chartes à des actes mettant sciemment en péril la sécurité ou le fonctionnement d'autres sites et des réseaux de télécommunications.

La simple accession à un système sans autorisation constitue un délit, même s'il n'en est résulté aucune altération des données ou fonctionnement dudit système.

ARTICLE 8 - Analyse et contrôle de l'utilisation des ressources

Pour des nécessités de maintenance, de gestion technique et de sécurité, l'utilisation des ressources du système d'informations et les échanges via le réseau sont analysés et contrôlés dans le respect de la législation applicable et des règles d'utilisation énoncées dans la présente charte.

Les services habilités de l'école national des chartes peuvent à tout moment assurer le contrôle du respect de ces obligations par les utilisateurs et les utilisatrices.

TITRE III - PROTECTION ET SECURITE

Article 9 - Protection des données personnelles

L'École nationale des chartes est vigilante à la protection des données personnelles de l'ensemble des utilisateurs et utilisatrices qui constitue une

priorité. Elle est soumise au règlement européen n°2016/679 dit « Règlement Général pour la protection des données personnelles » (RGPD) et à la loi n° 78-17 du 6 janvier 1978 dite « Informatique et libertés ». L'École nationale des chartes est donc responsable de traitement au sens du RGPD. Il s'agit de toute donnée à caractère personnel permettant directement ou indirectement l'identification des personnes physiques auxquelles elles s'appliquent.

La mise en place d'un traitement de données personnelles doit avoir fait l'objet d'une concertation en amont avec le Délégué à la protection des données et satisfaire aux textes législatifs et réglementaires susmentionnés.

Dans le cadre de la réalisation de ses missions, l'utilisateur ou l'utilisatrice est informé que l'École nationale des chartes doit collecter, stocker, utiliser et /ou archiver certaines de ses données personnelles.

Des transferts de certaines des données mentionnées ci-dessus peuvent être effectuées notamment en cas d'obligation légale : ministères, rectorat, URSSAF, commissaires aux comptes, mutuelle etc. sans que cette liste ne soit exhaustive.

Nonobstant l'alinéa précédent, les données personnelles sont traitées en interne par les services de l'École nationale des chartes et notamment par les services des ressources humaines, des systèmes d'information, de la scolarité, de la vie étudiante, de la communication et de la logistique.

Tout autre usage externe de ces données, notamment à des fins de communication, ne seront effectués qu'après information et si nécessaire avec le consentement de l'utilisateur ou de l'utilisatrice conformément à l'article 9 du RGPD.

Les types de traitements ainsi que de données personnelles utilisées sont spécifiés :

- En annexe B de la présente charte pour les personnels;

- En annexe C de la présente charte pour les élèves et étudiants, stagiaires de la formation continue.

Conformément à l'article 37 du RGPD, l'École nationale des chartes a désigné un délégué à la protection des données. Les utilisateurs et les utilisatrices peuvent faire valoir leurs droits d'accès, de rectification et, le cas échéant, d'effacement de leurs données personnelles :

- Par messagerie électronique : dpo@chartes.psl.eu ;

- Par courrier à : Ecole nationale des chartes – PSS – DPO/Affaires juridiques – 65 rue de Richelieu 75002 Paris.

En l'absence de réponse ou en cas de réponse négative, l'utilisateur ou

l'utilisatrice peut le cas échéant exercer une réclamation auprès de la commission nationale de l'informatique et des libertés (CNIL).

Article 10 - Protection informatique

La protection des systèmes d'informations s'appuie sur les dispositions légales qui prévoient notamment que sont interdits l'accès illicite (toute introduction dans un système d'informations par une personne non autorisée), le maintien frauduleux (maintien sur un SI après un accès illicite et après avoir pris conscience du caractère illicite de cet accès), l'entrave au système (toute perturbation volontaire du fonctionnement d'un système d'information), l'altération des données (toute suppression, modification, ou introduction de données « pirates » ou de logiciels parasites plus connus sous le nom de virus, chevaux de Troie, bombes logiques... avec la volonté de modifier l'état du système informatique les exploitant) ou encore le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions décrites ci-dessus.

Article 11 – Mesures de sécurité prises par l'École nationale des chartes

Au titre de la sécurité du SI et des TIC, l'École nationale des chartes définit le niveau d'accès de chaque utilisateur ou utilisatrice en fonction de son profil qui est établi en prenant en compte son statut, sa fonction, la nature de ses activités et ses besoins. L'École nationale des chartes limite pour chaque utilisateur ou utilisatrice l'accès aux ressources en fonction du niveau d'accès qui lui a été attribué. L'École nationale des chartes veille à ce que certaines ressources ne soient accessibles qu'aux personnes spécialement habilitées à cet effet.

Par ailleurs, L'École nationale des chartes peut interrompre, modifier ou supprimer tout ou partie des services et équipements, de manière temporaire ou définitive. L'utilisateur ou l'utilisatrice en sera informé par courriel.

Article 12 – Règles de sécurité que l'utilisateur doit respecter

Au titre de la sécurité du SI et des TIC, l'utilisateur ou l'utilisatrice doit garder strictement confidentiels ses codes d'accès (tout utilisateur ou utilisatrice doit être enregistré dans les bases de référence de l'École nationale des chartes et avoir obtenu des codes d'accès qui lui sont personnels et

confidentiels). Si, pour quelque raison que ce soit, l'utilisateur ou l'utilisatrice est informé(e) ou estime que ses codes d'accès ne sont plus confidentiels, il doit procéder dès que possible au changement de ces derniers ou en demander la modification au responsable du dispositif.

L'utilisateur ou l'utilisatrice ne doit pas utiliser les codes d'accès d'un autre utilisateur ou utilisatrice, ni chercher à les connaître. Il ou elle ne doit pas accéder ou tenter d'accéder à des ressources du SI et aux communications entre tiers pour lesquelles il ou elle n'a pas reçu d'habilitation explicite. Il ou elle ne doit pas utiliser les services qui lui sont offerts pour proposer ou rendre accessibles à des tiers des informations confidentielles ou des données dont le contenu serait contraire à la législation en vigueur.

La connexion au SI des matériels autres que ceux autorisés par l'École nationale des chartes ou encore l'installation, le téléchargement ou l'utilisation sur le SI des logiciels dont les droits de licence n'ont pas été acquittés sont strictement interdits.

Toute perturbation au bon fonctionnement du SI et du réseau par des manipulations anormales de matériel ou par l'introduction de logiciels parasites pourra faire l'objet d'une sanction disciplinaire.

Article 13 – Obligations d'information

L'École nationale des chartes porte à la connaissance de l'utilisateur ou l'utilisatrice tout élément susceptible de lui permettre d'apprécier le niveau de risque encouru dans l'utilisation du SI et des TIC.

L'utilisateur ou l'utilisatrice doit informer, sans délai, le RSSI de l'École nationale des chartes de tout dysfonctionnement constaté ou de toute anomalie constatée (intrusion, altération, destruction). Il ou elle est également tenu€ de signaler toute possibilité d'accès à une ressource qu'il ou elle aurait constaté et qui ne correspondrait pas à son habilitation.

Par ailleurs, conformément à l'article 40 du Code de procédure pénale : « Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au Procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs ».

Article 14 – Dispositions relatives à la maintenance et au contrôle

Pour assurer les opérations nécessaires de maintenance technique (corrective, évolutive ou préventive) le Centre de ressources informatique de l 'École

nationale des chartes peut réaliser des interventions, éventuellement à distance, sur les moyens informatiques et de communication électronique mis à disposition de l'utilisateur ou l'utilisatrice.

Toute information bloquante ou présentant une difficulté d'acheminement à son destinataire peut être isolée, voire supprimée si nécessaire. Une notification sera envoyée à l'utilisateur ou l'utilisatrice.

Dans le respect des dispositions légales et règlementaires, une surveillance et un contrôle de l'usage du SI et des TIC sont mis en place à des fins statistiques, de traçabilité, d'optimisation, de sécurité et de détection des abus, et plus particulièrement en vertu des obligations qui incombent à l'École nationale des chartes en tant que fournisseur d'accès, un dispositif d'historisation des données de connexions (conservées durant une année) pouvant être fournies en cas de requête judiciaire ou administrative.

Les personnels (et leurs responsables) chargés des opérations de maintenance et de contrôle sont soumis à une obligation de confidentialité, ils doivent respecter la vie privée et le secret de la correspondance des utilisateurs et des utilisatrices sous la réserve de l'obligation légale.

TITRE IV – DISPOSITIONS FINALES

Article 15 – Sanction du non-respect des dispositions de la charte

En cas de non-respect des dispositions de la présente charte, l'École nationale des chartes peut prendre toutes mesures conservatoires s'imposant à l'encontre d'un utilisateur ou d'une utilisatrice, notamment, la récupération du matériel, le retrait des données de connexion, sans préjudice d'éventuelles procédures disciplinaires ou pénales qui seraient engagées.

Article 16 – Entrée en vigueur de la charte

La présente charte entre en vigueur au premier jour suivant sa signature par le chef d'établissement.

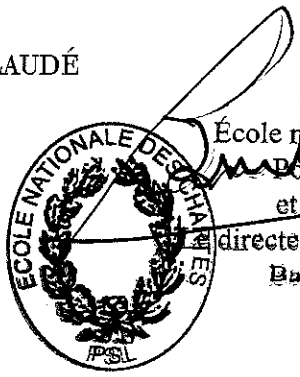
Article 17 - Modifications

Toutes modifications, ou adjonctions ou retraits ultérieures, à la présente charte seront soumis à la même procédure.

Le

L'administrateur provisoire de l'École nationale des chartes – PSL

Jean-François BALAUDÉ



École nationale des chartes
Pour la directrice
et par délégation
le directeur général des services
Baptiste BONDU

ANNEXE A – RESTRICTION D'UTILISATION D'INTERNET

Conformément à la charte relative à l'usage du système d'information et des technologies de l'information et de la communication de l'École nationale des chartes-PSL, l'utilisation d'internet constitutive d'infraction et de sanctions pénales est prévue par la loi.

ARTICLE 1 : LE PUBLIC CONCERNE

Sont concerné par les restrictions tous les publics se formant (élèves, étudiants, stagiaires de formation continue) à l'École nationale des chartes-PSL.

ARTICLE 2 : LES INFRACTIONS CONCERNEES

Les principales infractions concernées sont les infractions suivantes lorsqu'elles sont commises sur internet :

- Diffusion d'images violentes ou pédophiles
- Incitation à la violence
- Incitation à la haine raciale
- Incitation à la violence sexuelles et/ou sexiste
- Atteinte à la dignité humaine
- Harcèlement
- Apologies de crimes contre l'humanité
- Négation ou minimisation de crimes contre l'humanité
- Apologie du terrorisme
- Injures raciales
- Injures sexistes
- Diffamation
- Atteinte au droit à l'image et à la vie privée.

Sont également concernées les infractions suivantes :

- Le partage, le piratage, le téléchargement de films, documents, logiciels piratés
- Les jeux d'argent quel que soit le support
- La vente de médicaments interdits par la loi.

De plus, les restrictions de navigations concernent tout comportement impliquant un risque de sécurité :

- Diffusion de virus
- Spyware
- Phishing
- Codes malicieux
- Domaines Parkés
- Proxy, cache redirecteur

ARTICLE 3 : LES CONSEQUENCES

Le public concerné s'expose à des poursuites administratives et/ou judiciaires.

ANNEXE B – UTLISATION DES DONNEES PERSONNELLES DES PERSONNELS

Conformément aux articles 12, 13 et 14 du règlement général pour la protection des données, l'École nationale des chartes-PSL est tenue à une obligation de transparence vis-à-vis de ses personnels.

La présente annexe a pour objet de récapituler les finalités de traitement ainsi que les types de données récoltées dans le cadre de la gestion des ressources humaines.

L'École nationale des chartes-PSL doit assurer la sécurité des informations et garantir que seules les personnes habilitées en prennent connaissance qu'elles relèvent de la direction des ressources humaines, et sous certaines conditions, des représentants des personnels, des organisations syndicales, de la direction générale des services.

ARTICLE 1 : LE RESPONSABLE DE TRAITEMENT

Le responsable de traitement est le chef d'établissement de l'École nationale des chartes-PSL, sise 65 rue de Richelieu 75002 Paris, représentées par sa directrice.

La directrice a la possibilité de déléguer l'administration des données, mais reste responsable de leur utilisation.

ARTICLE 2 : FINALITE DU TRAITEMENT

Le traitement des données a pour objet d'assurer les fonctions de base de la gestion administratives de ses personnels.

ARTICLE 3 : SOUS-FINALITES DU TRAITEMENT

La gestion administrative recouvre cumulativement les situations de gestion suivantes :

- Gestion du dossier personnel individuel de chaque membre du personnel
- Outils informatiques nécessaires à l'exercice des fonctions
- Rémunérations, les différentes déclarations et le paiement des cotisations sociales afférentes
- Evaluations personnelles
- Suivi de carrière
- Formations professionnelles
- Le cas échéant, organisation de toute élection professionnelle, locale ou nationale.

ARTICLE 4 : BASE LEGALE DU TRAITEMENT

Le traitement et la conservation des données sont fondés sur les obligations légales de l'École nationale des chartes-PSL en tant qu'employeur public.

ARTICLE 5 : TYPES DE DONNEES TRAITEES

Les principales données concernées sont :

- Données relatives à l'identité : nom, prénom, civilité, date de naissance, nationalité, département de naissance, adresse administrative, photographie, le cas échéant, le permis de travail ;
- Situation personnelle de l'agent : : marié, pacsé, concubinage, enfants à charge, coordonnées des personnes à prévenir en cas d'urgence ;
- Situation professionnelle de l'agent et identification (NUMEN) : niveau d'études, photocopies des diplômes ;
- Eléments financiers et de protection sociale (RIB, INSEE, carte vitale)

ARTICLE 6 : TRANSFERT DE DONNEES

Ne sont autorisés que les transferts relevant de l'obligation légale vis-à-vis des administrations publiques. Les transferts hors de l'union européenne sont autorisées sous certaines conditions professionnelles.

ARTICLE 7 : CONSERVATION DES DONNEES

Les données personnelles et professionnelles de l'agent sont conservées le temps de sa présence à l'École nationale des chartes-PSL et pendant dix ans après sa sortie des effectifs de l'École. Le dossier sera ensuite soit conservé, soit définitivement supprimé conformément aux obligations règlementaires définies par le Code du patrimoine et le RGPD et les dispositions réglementaires d'archivage des données des agents publics.

ANNEXE C : UTLISATION DES DONNEES PERSONNELLLES DES ELEVES, ETUDIANTS ET STAGIAIRES DE FORMATION CONTINUE

Conformément aux articles 12, 13 et 14 du règlement général pour la protection des données, l'École nationale des chartes-PSL est tenue à une obligation de transparence vis-à-vis de ses élèves, étudiants et stagiaires de formation continue.

La présente annexe a pour objet de récapituler les finalités ainsi que les types de données récoltées dans le cadre de la formation.

L'École nationale des chartes-PSL doit assurer la sécurité des informations et garantir que seules les personnes habilitées en prennent connaissance.

ARTICLE 1 : LE RESPONSABLE DE TRAITEMENT

Le responsable de traitement est le chef d'établissement de l'École nationale des chartes-PSL, sise 65 rue de Richelieu 75002 Paris représentée par sa directrice.
La directrice a la possibilité de déléguer l'administration des données, mais reste responsable de leur utilisation.

ARTICLE 2 : FINALITE DU TRAITEMENT

Le traitement des données a pour objet d'assurer les fonctions de base de la gestion administratives et pédagogique des élèves, étudiants et stagiaires, pour les diplômes directement opérés par l'École nationale des chartes-PSL. Il doit également permettre de conserver un contact avec ces personnes au-delà de leur scolarité.

ARTICLE 3 : SOUS-FINALITES DU TRAITEMENT

La gestion administrative et pédagogique recouvre cumulativement les situations de gestion suivantes :

- Les inscriptions administratives et pédagogiques
- L'emploi du temps et le contrôle de l'assiduité
- Les relevés de notes
- L'obtention du diplôme
- Les stages, projets de césure ou autre situation pédagogique prévue par la direction des études

Le contact après la scolarité concerne les actes suivants :

- Suivi de l'insertion professionnelle ;
- Proposition d'offres d'emploi et de stages ;
- Inscription dans un réseau d'anciens ;

- Information sur la vie et les projets de l'École ;
- Appels à la générosité au bénéfice de l'École.

ARTICLE 4 : BASE LEGALE DU TRAITEMENT

Le traitement et la conservation des données sont fondés sur les obligations légales de l'École nationale des chartes-PSL en tant qu'établissement d'enseignement supérieur.

ARTICLE 5 : TYPES DE DONNEES TRAITEES

Les principales données concernées sont celles collectées au moment de l'inscription de l'élève, de l'étudiant ou du stagiaire :

- Données relatives à l'identité : nom, prénom, civilité, date de naissance, nationalité, département de naissance, adresse administrative, photographie d'identité, adresse mail, numéro de téléphone ;
- Situation personnelle (et celle des responsables légaux, si mineurs) ;
- Noms et coordonnées des parents (pour les élèves, étudiants et doctorants) ;
- Situation scolaire et universitaire de l'élève ou de l'étudiant, y compris les données administratives et/ou pédagogiques récoltées avant l'inscription de l'École nationale des chartes-PSL : : relevé de notes, diplômes, stages ;
- Situation économique (bourse d'études, échelon, attestation CVEC)

ARTICLE 6 : TRANSFERT DE DONNEES

Ne sont autorisés que les transferts relevant de l'obligation légale vis-à-vis des administrations publiques. Les transferts hors de l'union européenne sont autorisées sous certaines conditions pédagogiques dont les stages à l'étranger.

ARTICLE 7 : CONSERVATION DES DONNEES

Les données administratives et pédagogiques sont conservées le temps de sa présence à l'École nationale des chartes-PSL, puis 10 ans si les documents récapitulatifs ont été conservés, ou sinon 50 ans à compter de l'obtention du diplôme ou du départ de l'établissement. Le dossier sera ensuite conservé conformément aux obligations règlementaires définies par le Code du patrimoine et le RGPD et transmises aux archives nationales pour y être conservées indéfiniment.

ANNEXE D - LE REGISTRE DES ACTIVITES DE TRAITEMENT

Le registre est prévu par l'article 30 du RGPD. Il participe à la documentation de la conformité. Au-delà de la réponse à l'obligation prévue par l'article 30 du RGPD, le registre est un outil de pilotage et de démonstration de conformité au RGPD. Il permet en 1er lieu de documenter les traitements de données utilisés par l'Ecole nationale des chartes-PSL. Il peut être constitue sous format papier ou numérique.

ARTICLE 1 : DOCUMENT DE RECENSEMENT ET D'ANALYSE

Le registre de traitement des données permet d'identifier précisément :

- Les parties prenantes (représentant, sous-traitants, co-responsables, etc.) qui interviennent dans le traitement des données,
- Les catégories de données traitées,
- À quoi servent ces données (ce que l'Ecole en fait), qui accède aux données et à qui elles sont communiquées,
- Durée de conservation,
- Sécurisation des données.

ARTICLE 2 – LA FICHE REGISTRE

Le registre du responsable de traitement doit recenser l'ensemble des traitements mis en œuvre par l'Ecole. Une fiche de registre doit être établie pour chacune des activités de l'Ecole nationale des chartes -PSL.
Pour chaque activité de traitement, la fiche de registre doit comporter au moins les éléments suivants :

1. Le cas échéant, le nom et les coordonnées du responsable conjoint du traitement mis en œuvre ;
2. Les finalités du traitement, l'objectif en vue duquel sont collectées ces données ;
3. Les catégories de personnes concernées (étudiants, personnels, etc.) ;
4. Les catégories de données personnelles (exemples : identité, situation familiale, économique ou financière, données bancaires, données de connexion, donnés de localisation, etc.) ;
5. Les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les sous-traitants
6. Les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale et, dans certains cas très particuliers, les garanties prévues pour ces transferts ;
7. Les délais prévus pour l'effacement des différentes catégories de données, c'est-à-dire la durée de conservation, ou à défaut les critères permettant de la déterminer ;
8. Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles mises en œuvre.

École
nationale
des
chartes

Conseil technique rattaché à la Direction générale des services

DÉCISION PORTANT NOMINATION DE LA DÉLÉGUÉE À LA PROTECTION DES DONNÉES DE L'ÉCOLE NATIONALE DES CHARTES

La directrice de l'École nationale des chartes

Paris, le 30 septembre 2019

Vu 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, et abrogeant la directive 95/46/CE ;
Vu la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles ;

DÉCIDE

Article 1 : Mme Egina SANTOROMITO, conseillère technique auprès du directeur général des services de l'École nationale des chartes est nommée déléguée à la protection des données de l'École nationale des chartes. Les missions de la déléguée à la protection des données sont précisées par lettre de mission.

Article 2 : Le directeur général des services est chargé de l'exécution de la présente décision.

La directrice de l'École

Michelle BUBENICEK

ÉCOLE NATIONALE DES CHARTES
La Directrice

PSL

Membre du campus Condorcet

65, rue de Richelieu
F-75002 Paris
T +33 (0)1 55 42 75 00
directeur@ chartes.psl.eu

Bibliothèque
12, rue des Petits-Champs
F-75002 Paris
T + 33 (0)1 55 42 88 69
bibliotheque@chartes.psl.eu

www.chartes.psl.eu

Charte d'utilisation des ressources du système d'information

TITRE I – OBJET ET CHAMP D'APPLICATION

ARTICLE 1 – Objet

La présente charte définit les droits et obligations des utilisateurs et utilisatrices du Système d'Information (SI) et des Technologies de l'Information et de la Communication (TIC) (matériels ou immatériels) mis à disposition par PSL – Paris Sciences et Lettres. Elle intègre et décline les dispositions légales et réglementaires qui s'imposent à PSL – Paris Sciences et Lettres et aux utilisateurs et utilisatrices.

Elle est complétée par des annexes, notamment par :

- Annexe A – Restrictions d'utilisation d'internet ;
- Annexe B – Politique de confidentialité des données des personnels ;
- Annexe C – Politique de confidentialité des données des étudiants et étudiantes.

ARTICLE 2 - Domaine d'application

1. Utilisateurs et utilisatrices

On désigne sous le terme « utilisateur » et « utilisatrice » toute personne physique ou morale, sans exception, disposant d'un accès, utilisant les ressources du système d'Information mis à disposition par PSL ou intervenant sur ledit système.

Les règles et procédures prévues dans la présente charte s'imposent à tout utilisateur et utilisatrice quel que soit son statut (personnels, agents stagiaires, enseignants, étudiants, vacataires, chercheurs, prestataires externes intervenant en sous-traitance, usagers, personnes invitées … sans que cette liste ne soit exhaustive) ou sa situation géographique vis-à-vis de PSL.

2. Ressources du système d'information

On entend par Système d'Information (SI) et Technologies de l'Information et de la Communication (TIC) l'ensemble des moyens matériels et immatériels, des logiciels, des bases de données et des réseaux de communication pouvant être mis à disposition des utilisateurs et des utilisatrices.

L'accès à cet ensemble à distance, par un poste fixe ou par l'informatique « nomade » (assistants personnels, ordinateurs portables, smartphones, clé USB, accès au web, espace de stockage…), relève également de la présente charte. Il en est de même de toute nouvelle technologie de l'information et de communication mise à disposition par PSL– Paris Sciences et Lettres.

3. PSL – Paris Sciences et Lettres

On entend par PSL – Paris Sciences et Lettres tant la Fondation de coopération scientifique Paris Sciences et Lettres que l'Université Paris Sciences et Lettres.

4. Le responsable sécurité système d'information (RSSI) et responsable d'application (RA)

Des mesures de contrôle et de suivi sont mises en œuvre dans le strict respect des principes de transparence et de proportionnalité et de respect du RGPD, ceci uniquement à des fins de sécurité et de vérification du bon accès et usage du SI.

Ces mesures ont pour objectifs :

- De garantir le bon fonctionnement du SI et la continuité de service ;
- De contrôler le respect des règles d'utilisation et de sécurité du SI ;
- De pouvoir identifier et, le cas échéant, sanctionner des comportements ou usages abusifs, ou qui ne respecterait pas les dispositions légales ;

- De pouvoir répondre aux requêtes des autorités publiques habilitées (services de police, autorités judiciaires…).

Ces mesures pourront prendre les formes suivantes :

- **Traçabilité** :

Pour satisfaire aux obligations légales qui lui incombent, et par exemple apporter la preuve, du bon usage du SI mis à la disposition des utilisateurs et utilisatrices, PSL peut mettre en œuvre des outils de traçabilité tels que des journaux de connexions de l'ensemble du SI.
Les informations peuvent être conservées pour une durée limitée, qui dépendent des applications ou logiciels concernés.

- **Filtrage** :

Pour satisfaire aux obligations légales qui lui incombent et afin de prévenir tout usage illicite du SI, PSL se réserve le droit de mettre en place des outils de filtrage permettant d'analyser les conditions d'utilisation de ces moyens, d'interdire tel ou tel protocole, ou encore de restreindre certaines catégories de sites internet ou d'application.

- **Scan informatique** :

PSL peut procéder à des opérations de scan des systèmes d'information et de communication.
Les outils de scan informatique n'ont pas pour objet l'ouverture des éléments identifiés ou individuels. Ils permettent à PSL de disposer d'un dispositif d'alerte prudentiel et préventif du SI.

Les documents, dossiers, courriers électroniques, pièces jointes, etc. identifiés comme « PRIVE » sont exclus de ce dispositif sauf dans le cadre des dispositions légales particulières de la jurisprudence en la matière et de la présente charte.

- **Contrôle et audit** :

Des opérations de contrôle et d'audit portant sur la régularité de l'utilisation du SI et son niveau de sécurité, peuvent être mises en œuvre à PSL.
L'utilisation des moyens et ressources informatiques et numériques pourra faire l'objet d'une surveillance afin de détecter toute utilisation non conforme, malveillante ou d'optimiser cette même utilisation ou encore de mener des analyses statistiques.

- **Maintenance** :

La mise à disposition de moyens et ressources informatiques et numériques implique nécessairement des opérations de maintenance technique (maintenance corrective, maintenance préventive ou évolutive), et ce, pour assurer le bon fonctionnement et la sécurité de ceux-ci.
Ces opérations peuvent prendre la forme d'une intervention d'une « personne habilitée » soit sur site, soit à distance, conduisant alors cette personne à effectuer une « prise en main à distance », dont l'utilisateur ou l'utilisatrice doit être informé.e.
En aucun cas, ces opérations, quel que soit leur mode opératoire, ne justifient le fait pour l'utilisateur ou l'utilisatrice de divulguer ses moyens d'authentification.
Dans ce cadre, la « personne habilitée » peut être amenée à prendre connaissance de l'ensemble des éléments présents sur le poste ou le matériel nomade de l'utilisateur ou de l'utilisatrice ainsi que des données de connexion, qu'il s'agisse d'un usage professionnel ou privé.

Pour ce faire, le RA ou RSSI, assure notamment l'enregistrement, la sauvegarde et la gestion des traces et journaux d'évènements du SI, pendant la durée légale de conservation. Pour exercer leurs fonctions, le RSSI et RA pourront accéder aux informations relatives aux utilisateurs et utilisatrices, dans les conditions définies par la charte et par la réglementation applicable.
Ainsi seuls le RSSI et RA sont autorisés à prendre la main à distance sur les équipements mis à disposition par PSL aux utilisateurs et utilisatrices afin de résoudre les problèmes ou dysfonctionnements.

Les missions des RA ou RSSI portent sur la qualité et la sécurité du SI : ils et elles sont garant.e.s du bon fonctionnement et de la sécurité des ressources ainsi que la disponibilité des informations et du SI.

ARTICLE 3 - Finalité de l'utilisation du SI

1. Usage à des fins pédagogiques, scientifiques, de recherche ou professionnelle

L'accès par un utilisateur ou une utilisatrice aux SI est considéré comme un usage réalisé dans le cadre de l'activité professionnelle, pédagogique ou scientifique, et de recherche de l'utilisateur ou utilisatrice dans les limites des habilitations / autorisations qui lui sont accordées.

2. Usage à des fins privées

Un usage en dehors des usages professionnels, pédagogiques ou scientifiques ou de recherche du SI, dans le cadre des nécessités de la vie courante et familiale, est toléré par PSL de manière ponctuelle, et raisonnée et à condition que cet usage soit strictement conforme à la législation et la réglementation applicables, ainsi qu'à la présente charte.

À cet égard, l'usage privé ne doit pas :

- porter préjudice à l'activité de PSL ou de ses utilisateurs et utilisatrices ;
- être susceptible d'affecter le bon fonctionnement ou mettre danger la sécurité du SI.
- porter atteinte aux obligations qui incombent aux utilisateurs compte tenu de leur statut et notamment, les obligations de dignité, de loyauté, de discrétion, de neutralité ou de réserve ;
- porter atteinte ou être susceptible d'engager la responsabilité de PSL;
- poursuivre un but lucratif;
- porter atteinte à l'image de marque ou à la réputation de PSL.

Ainsi, seront présumés privés les fichiers et messages qui, lors de leur création, de leur traitement ou de leur conservation auront été clairement identifiés par l'utilisateur ou l'utilisatrice de la manière décrite ci-dessous :

- **Pour les messages** : tant pour les messages émis que reçus, le message doit mentionner une indication permettant de l'identifier comme privé (exemple : « personnel ») ;

- **Pour les fichiers** : les noms des fichiers doivent mentionner une indication permettant de les identifier comme privé (exemple : « personnel ») et ils doivent être conservés dans des répertoires spécifiques permettant également de les identifier comme privés.

Aucun fichier à usage professionnel, ne peut être nommé « privé » ou « personnel ».

Enfin, les communications émises ou reçues dans le cadre d'une activité protégée par des dispositions légales (exemple : secret médical) sont également considérées comme privées au sens de la présente charte, même si elles ne sont pas explicitement identifiées comme telles.
Tous les autres messages et fichiers sont considérés comme professionnels au sens de ladite charte.

TITRE II – UTILISATION ET BON USAGE DES SYSTEMES

ARTICLE 4 - Règles d'utilisation du matériel

L'accès aux réseaux et aux différents systèmes informatiques est strictement personnel et ne peut en aucun cas être cédé, même temporairement, à un tiers. Il peut être retiré à tout moment. Toute autorisation prend fin lors de la cessation de l'activité professionnelle, scolaire, d'enseignement et de recherche pour laquelle elle a été initialement concédée.

Tout utilisateur ou utilisatrice est responsable de l'usage qu'il ou elle fait des ressources du SI auxquelles il ou elle a accès. L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation ou leur détournement à des fins personnelles.
L'utilisateur ou l'utilisatrice a la charge, à son niveau, de contribuer à la sécurité générale du système d'information de PSL. Il ou elle doit notamment appliquer les recommandations de sécurité de PSL mentionnées dans la présente charte, assurer la protection de ses informations en utilisant les différents moyens de sécurité mis à sa disposition, en choisissant notamment des mots de passe sûrs et gardés secrets

et être responsable du bon usage de ses droits.

En outre, l'utilisateur ou l'utilisatrice se doit de signaler toute anomalie qu'il peut constater au responsable de la sécurité des systèmes d'information (RSSI) de PSL. Il doit veiller à ne pas installer de logiciels, ni contourner ses restrictions d'utilisation. En dehors d'autorisations exceptionnelles et spécifiques, seules les équipes de la Direction des systèmes d'informations sont autorisées à installer les logiciels dûment acquis par PSL.

Afin d'éviter toute usurpation d'identité, l'utilisateur ou l'utilisatrice doit veiller à ne pas laisser son matériel sans surveillance et sans se déconnecter (session, comptes…) en laissant des ressources ou services accessibles. Il doit également veiller à ne pas utiliser ou essayer d'utiliser des droits autres que les siens, de masquer sa véritable identité ou d'usurper celle d'autrui.

ARTICLE 5 – Règles d'utilisation des services internet et messagerie ou messagerie instantanée

Il appartient à l'utilisateur ou à l'utilisatrice de procéder au stockage éventuel de ses fichiers à caractère privé dans un espace prévu explicitement à cet effet (espace exclusivement dénommé « privé » ou « personnel ») dont la responsabilité et la sauvegarde lui incombent. Cet espace est à localiser sur les disques durs du poste informatique et autres périphériques de l'utilisateur ou de l'utilisatrice et en aucun cas sur les serveurs de fichiers (lecteurs réseaux nominatifs ou communs) ou sur un espace virtuel de stockage mis à sa disposition par PSL. Il lui revient également d'identifier explicitement ses courriels à caractère strictement privé, en ajoutant « personnel » dans l'objet.

Si le moyen de communication utilisé ne comporte pas de champ « objet » (chat, messagerie instantanée, sms…), le message à caractère non professionnel doit débuter par le terme « Personnel ».

Afin d'assurer la continuité de service, l'utilisateur ou l'utilisatrice doit privilégier le dépôt de ses fichiers de travail sur des zones partagées par les membres de son service ou de son équipe.

En cas de départ, ou d'absence prolongée, l'utilisateur ou l'utilisatrice informe PSL des modalités permettant l'accès aux ressources mises spécifiquement à sa disposition. En tout état de cause les données non situées dans un espace identifié comme privé, sont considérées comme appartenant à PSL qui pourra en disposer.

L'utilisateur ou l'utilisatrice doit veiller à ne pas se connecter ou essayer de se connecter sur un serveur, interne ou externe, autrement que par les dispositions prévues par la politique de sécurité des systèmes d'Information (PSSI) de PSL ou sans y être autorisé. Il ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède. L'usage des ressources qui sont confiées à l'utilisateur ou l'utilisatrice ne doit pas être contraire à la réglementation en vigueur (ex : téléchargement illégal d'œuvres de l'esprit, visionnage illégal de programmes audiovisuels en « streaming ») Enfin, il ou elle doit veiller à ne pas utiliser ces ressources pour proposer ou rendre accessibles aux tiers des données et informations confidentielles ou contraires à la législation en vigueur.

L'utilisateur ou l'utilisatrice doit faire preuve de la plus grande correction et discrétion à l'égard de ses interlocuteurs ou interlocutrices dans les échanges et notamment pour les courriers, forums de discussions, intranet, etc. A cet égard, il doit notamment veiller à ne pas émettre d'opinions susceptibles de porter préjudice à PSL.

PSL ne peut être tenu pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se conforme pas à ces règles.

Les usages relevant de l'activité des organisations syndicales et de leurs représentants sont régis par les dispositions législatives et règlementaires en vigueur. Dans ce cadre, les listes de diffusion syndicales ainsi que les pages syndicales ouvertes sur le site de type intranet ou de réseau social interne sont libres d'expression, des restrictions ne pouvant intervenir que conformément à la législation en vigueur.

Les listes de diffusion à destination des étudiants et étudiantes ou des enseignants et enseignantes sont réservées à l'équipe de direction et de la scolarité de PSL. Elles sont utilisées pour communiquer des informations liées à la scolarité et à la pédagogie. Leur usage par tout autre utilisateur et/ou à toute autre fin, devra avoir fait l'objet d'une autorisation préalable de l'administration de PSL.

ARTICLE 6 – Règles d'utilisations des espaces de stockages

PSL s'engage dans la lutte contre les dépenses énergétiques et l'usage non responsable des espaces de stockage, transmission de fichiers volumineux, ou toutes actions pouvant conduire à des comportements nos respectueux de l'environnement.

Les utilisateurs et utilisatrices devront donc :

- Utiliser les espaces de stockages collectifs et non individuels, voire canaux d'outils collaboratifs dédiés.
- Supprimer ou archiver les informations non essentielles à leurs activités quotidiennes
- Limiter la duplication dans différents espaces d'une même information
- Respecter les quotas sur les espaces de stockage (boîte mail, et espace nominatif) en vigueur à PSL

ARTICLE 7 - Obligation de conserver l'intégrité des Informations

L'utilisateur ou l'utilisatrice doit respecter les procédures d'hébergement des Informations, dans la mesure où elles sont définies par PSL et par exemple :

- l'utilisateur ou l'utilisatrice doit enregistrer régulièrement les informations qu'il exploite, qu'il crée ou qu'il ou elle transforme dans les espaces prévus à cet effet. Il ou elle est par ailleurs responsable personnellement de la sauvegarde de ses données stockées localement sur ses appareils ;
- l'utilisateur ou utilisatrice doit verrouiller ou déconnecter ses équipements en cas d'absence même temporaire ;
- l'utilisateur ou utilisatrice ne doit pas déplacer, dupliquer ou détruire les Informations sur lesquelles son statut et ses missions le conduisent à intervenir avant de s'être assuré que cela ne porte aucun préjudice à PSL ou autre utilisateur ou utilisatrice.

ARTICLE 8 - Continuité de service

Sans préjudice des dispositions prévues ci-dessus, afin d'assurer une continuité de service, dans l'hypothèse où l'utilisateur ou utilisatrice change de statut au sein de PSL ou quitte PSL, il ou elle devra suivre la procédure applicable à la transmission des informations ou données qu'il ou elle détient, par exemple sur ses espaces partagés, sa messagerie ou les équipements mis à disposition par PSL.
Toute opération d'effacement d'informations autre que « privé » devra recevoir de manière générale ou spécifique, l'autorisation de la direction générale des services (DGS), de la DSI ou du responsable hiérarchique ou fonctionnel.

Les responsables des applications ou du SI sont autorisés à réaliser des sauvegardes et archivages de tout ou partie du SI, y compris ceux hébergeant les données des utilisateurs ou utilisatrices, afin d'assurer la continuité de service.

ARTICLE 9 - Confidentialité et protection des libertés individuelles

L'accès par l'utilisateur ou l'utilisatrice aux informations et documents conservés sur les systèmes d'information doit être limité à ceux qui lui sont propres, et ceux qui sont publics ou partagés.

Il est strictement interdit de prendre connaissance d'informations détenues par d'autres utilisateurs ou utilisatrices soit sur leur messagerie soit sur leur session qui leur sont personnelles, quand bien même ceux-ci ne les auraient pas explicitement protégées.

Il pourra être dérogé à cette règle pour des motifs impérieux de bon fonctionnement du service et notamment afin d'assurer leur bonne continuité ou encore la sécurité des systèmes d'information ainsi que pour tout autre cas autorisé par les dispositions législatives et réglementaires en vigueur. La décision devra être prise par l'employeur ou son représentant dans le cas des personnels, et du chef d'établissement ou de son délégataire dans le cas des étudiants et étudiantes et enseignants et enseignantes.

L'utilisateur ou l'utilisatrice, s'interdit de noter dans le système d'information des informations prohibées relatives à la vie privée des tiers, collaborateurs et collaboratrices, étudiants et étudiantes, enseignants et enseignantes, ainsi que d'émettre des opinions pouvant avoir un caractère injurieux, raciste, pornographique ou diffamatoire.

ARTICLE 10 - Respect du droit de propriété intellectuelle et de la vie privée

Dans le cadre professionnel, pédagogique ou scientifique des outils techniques d'enregistrements vidéo et sonores sont mis en place.
Les utilisateurs et les utilisatrices doivent respecter les dispositions du code de la propriété intellectuelle.

À ce titre, ils doivent notamment utiliser les logiciels dans les conditions des licences souscrites. Il est strictement interdit de 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 sans avoir obtenu l'autorisation du ou des titulaire(s) des droits (les logiciels et documents « libres » relèvent aussi de ces dispositions).

De la même façon, les marques ne peuvent être utilisées sans autorisation du ou des propriétaire(s).

L'auteur ou l'autrice d'une contrefaçon engage directement sa responsabilité, il peut être poursuivi devant les tribunaux ainsi que le cas échéant, la personne morale qui l'emploie.

Aucune captation (cours, réunions, forum…sans que cette liste ne soit exhaustive) ne doit porter atteinte à l'intégrité, la dignité ou à l'image des personnes concernées, et ne peut être utilisée à une fin autre que celle à laquelle les participants ont librement consenti. Toute utilisation commerciale non autorisée au préalable est proscrite

Les utilisateurs et utilisatrices sont informé.e.s de l'existence de ces outils d'enregistrement, mais il est impératif d'indiquer son usage à un utilisateur ou utilisatrice.

Dans le cadre des enseignements à distance, les cours enregistrés pourront être utilisés à des fins pédagogiques dans le seul but d'être visionnés et revisionnés par les étudiants régulièrement inscrits.

Conformément aux articles 226-1, 226-2 et 226-8 du code pénal, toute personne qui contreviendrait aux dispositions qui précèdent s'expose à des sanctions pénales si elle diffuse, partage, ou communique par n'importe quel moyen, ces images, animées ou non, et/ou les paroles en dehors de ce cadre universitaire.

ARTICLE 11 - Préservation de l'intégrité

L'utilisateur ou l'utilisatrice s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes d'information et des réseaux notamment par des manipulations anormales du matériel ou par l'introduction de logiciels malveillants.

L'implantation, l'utilisation, le développement ou la diffusion de programmes mettant en cause l'intégrité des systèmes sont prohibés. Il est interdit de se livrer depuis des systèmes appartenant à PSL à des actes mettant sciemment en péril la sécurité ou le fonctionnement d'autres sites et des réseaux de télécommunications.

La simple accession à un système sans autorisation constitue un délit, même s'il n'en est résulté aucune altération des données ou fonctionnement dudit système.

TITRE III - PROTECTION ET SECURITE

Article 12 - Protection des données personnelles

PSL est vigilante à la protection des données personnelles de l'ensemble des utilisateurs et utilisatrices ce qui constitue une priorité. Elle est soumise au règlement européen n°2016/679 dit « Règlement Général pour la protection des données personnelles » (RGPD) et à la loi n° 78-17 du 6 janvier 1978 dite « Informatique et libertés ». PSL est donc responsable de traitement au sens du RGPD. Il s'agit de toute donnée à caractère personnel permettant directement ou indirectement l'identification des personnes physiques auxquelles elles s'appliquent.

La mise en place d'un traitement de données personnelles doit avoir fait l'objet d'une concertation en amont avec le Délégué à la protection des données et satisfaire aux textes législatifs et réglementaires susmentionnés.

Dans le cadre de la réalisation de ses missions, l'utilisateur ou l'utilisatrice est informé que PSL doit collecter, stocker, utiliser et /ou archiver certaines de ses données personnelles.

Des transferts de certaines des données mentionnées ci-dessus peuvent être effectuées notamment en cas d'obligation légale : Ministères de l'économie et du budget et de l'enseignement supérieur, rectorat, URSSAF, commissaires aux comptes, mutuelle…

Nonobstant l'alinéa précédent, les données personnelles sont traitées en interne par les services de PSL et notamment les services des ressources humaines, des systèmes d'information, la scolarité, vie étudiante, la communication et de la logistique et la direction des affaires juridiques.

Tout autre usage externe de ces données, notamment à des fins de communication, ne seront utilisées qu'après information et si nécessaire avec le consentement de l'utilisateur ou de l'utilisatrice conformément à l'article 9 du RGPD.

Conformément à l'article 37 du RGPD, PSL a désigné un délégué à la protection des données. Les utilisateurs et les utilisatrices peuvent faire valoir leurs droits d'accès, de rectification et, le cas échéant, d'effacement de leurs données personnelles :

- Par messagerie électronique : donnees.personnelles@psl.eu ;
- Par courrier à : Université PSL – DPO/Affaires juridiques – 60 rue Mazarine 75006 Paris.

En l'absence de réponse ou en cas de réponse négative, l'utilisateur ou l'utilisatrice peut le cas échéant exercer une réclamation auprès de la commission nationale de l'informatique et des libertés (CNIL).

Article 13 - Protection informatique

La protection des systèmes d'informations s'appuie sur les dispositions légales qui prévoient notamment que sont interdits l'accès illicite (toute introduction dans un système d'informations par une personne non autorisée), le maintien frauduleux (maintien sur un SI après un accès illicite et après avoir pris conscience du caractère illicite de cet accès), l'entrave au système (toute perturbation volontaire du fonctionnement d'un système d'information), l'altération des données (toute suppression, modification, ou introduction de données « pirates » ou de logiciels parasites plus connus sous le nom de virus, chevaux de Troie avec la volonté de modifier l'état du système informatique les exploitant) ou encore le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions décrites ci-dessus.

Article 14 – Mesures de sécurité prises par PSL

Au titre de la sécurité du SI et des TIC, PSL définit le niveau d'accès de chaque utilisateur ou utilisatrice en fonction de son profil qui est établi en prenant en compte son statut, sa fonction, la nature de ses activités et

ses besoins. PSL limite pour chaque utilisateur ou utilisatrice l'accès aux ressources en fonction du niveau d'accès qui lui a été attribué. PSL veille à ce que certaines ressources ne soient accessibles qu'aux personnes spécialement habilitées à cet effet.

Par ailleurs, PSL peut interrompre, modifier ou supprimer tout ou partie des services et équipements, de manière temporaire ou définitive. L'utilisateur ou l'utilisatrice en sera informé par courriel.

Article 15 – Règles de sécurité que l'utilisateur doit respecter

Au titre de la sécurité du SI et des TIC, l'utilisateur ou l'utilisatrice doit garder strictement confidentiels ses codes d'accès (tout utilisateur ou utilisatrice doit être enregistré dans les bases de référence de PSL et avoir obtenu des codes d'accès qui lui sont personnels et confidentiels). Si, pour quelque raison que ce soit, l'utilisateur est informé ou estime que ses codes d'accès ne sont plus confidentiels, il doit procéder dès que possible au changement de ces derniers ou en demander la modification au responsable du dispositif.

L'utilisateur ou l'utilisatrice ne doit pas utiliser les codes d'accès d'un autre utilisateur ou utilisatrice, ni chercher à les connaître. Il ne doit pas accéder ou tenter d'accéder à des ressources du SI et aux communications entre tiers pour lesquelles il n'a pas reçu d'habilitation explicite. Il ne doit pas utiliser les services qui lui sont offerts pour proposer ou rendre accessibles à des tiers des informations confidentielles ou des données dont le contenu serait contraire à la législation en vigueur.

La connexion au SI des matériels autres que ceux autorisés par PSL ou encore l'installation, le téléchargement ou l'utilisation sur le SI des logiciels dont les droits de licence n'ont pas été acquittés sont strictement interdits. Toute perturbation au bon fonctionnement du SI et du réseau par des manipulations anormales de matériel ou par l'introduction de logiciels parasites pourra faire l'objet d'une sanction disciplinaire.

Article 16 – Obligations d'information

PSL porte à la connaissance de l'utilisateur ou l'utilisatrice tout élément susceptible de lui permettre d'apprécier le niveau de risque encouru dans l'utilisation du SI et des TIC.

L'utilisateur ou l'utilisatrice doit informer, sans délai, le RSSI de PSL de tout dysfonctionnement constaté ou de toute anomalie constatée (intrusion, altération, destruction, vol ou perte de matériel). Il ou elle est également tenu.e de signaler, toute possibilité d'accès à une ressource qu'il aurait constaté et qui ne correspondrait pas à son habilitation.
Enfin, il ou elle devra impérativement, et dans les plus brefs délais, informer le RSSI de PSL de toutes dégradations, pertes, vols des ressources du SI mis à sa disposition, et se doit de faire les démarches utiles (déclaration de vol auprès des autorités compétentes…) et de fournir à PSL tous les justificatifs permettant de réalisées les opérations de sauvegardes, blocages ou démarches auprès de l'assurance.

Par ailleurs, conformément à l'article 40 du Code de procédure pénale : « Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au Procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs ».

Article 17 – Dispositions relatives à la maintenance et au contrôle

Pour assurer les opérations nécessaires de maintenance technique (corrective, évolutive ou préventive) la Direction des systèmes d'informations de PSL peut réaliser des interventions, éventuellement à distance, sur les moyens informatiques et de communication électronique mis à disposition de l'utilisateur ou l'utilisatrice.

Toute information bloquante ou présentant une difficulté d'acheminement à son destinataire peut être isolée, voire supprimée si nécessaire. Une notification sera envoyée à l'utilisateur ou l'utilisatrice.

Dans le respect des dispositions légales et règlementaires, une surveillance et un contrôle de l'usage du SI et des TIC sont mis en place à des fins statistiques, de traçabilité, d'optimisation, de sécurité et de détection des abus, et plus particulièrement en vertu des obligations qui incombent à PSL en tant que fournisseur d'accès, un dispositif d'historisation des données de connexions (conservées durant une année) pouvant être fournies en cas de requête judiciaire ou administrative.

Les personnels (et leurs responsables) chargés des opérations de maintenance et de contrôle sont soumis à une obligation de confidentialité, ils doivent respecter la vie privée et le secret de la correspondance des utilisateurs et des utilisatrices sous la réserve de l'obligation légale.

Article 18 – Les déplacements à l'étranger

En cas de doute avant le déplacement, l'utilisateur ou l'utilisatrice peut prendre conseil auprès du RSSI afin de sécuriser au mieux son matériel SI et TIC.
Pendant le déplacement à l'étranger pour des raisons personnelles ou professionnelles, une vigilance particulière s'impose. L'utilisateur ou l'utilisatrice doit notamment respecter les règles suivantes :

- éviter dans la mesure du possible le stockage de données sensibles ;
- privilégier l'accès aux données sensibles via des connexions sécurisées (VPN) plutôt qu'un stockage sur les équipements nomades de type ordinateur portable, smartphone ;
- sauvegarder les données et conserver la sauvegarde en lieu sûr ;
- ne pas se séparer de son matériel.

L'utilisateur ou l'utilisatrice n'est pas autorisé.e à utiliser d'appareils offerts (tablette, ordinateur, clé USB, etc.) : ces cadeaux contiennent souvent des logiciels malveillants.

Pour les mêmes raisons, il est impérieux de ne pas connecter les appareils sur des postes ou réseaux informatiques peu fiables. L'accès à internet dans les cybercafés, les hôtels ou les lieux publics ne garantit aucune confidentialité. La vigilance est donc de mise lors d'une connexion et le pare-feu doit rester actif. Il est rappelé que le réseau Eduroam est présent notamment dans les aéroports internationaux.

De même, il est déconseillé de recharger les équipements dans les bornes électriques libre-service. Ce type de borne peut copier vos données.
Rendre compte au RSSI dans les plus brefs délais de toute anomalie sur le SI ou le TIC ou comportement suspect de la part des autorités ou autre à l'étranger.

En cas d'indisponibilité, l'utilisateur ou l'utilisatrice peut rapprocher du consulat français avant d'entamer toute démarche auprès des autorités locales.

Au retour de la mission, en cas de saisie du matériel (police aux frontières, accueil d'une organisation, etc.) durant le déplacement ou si des doutes existent sur l'intégrité de l'un d'eux, il est conseillé de changer les mots de passe et de confier les équipements utilisés au RSSI.

Article 19 – Télétravail

Conformément à l'arrêté du 22 juillet 2016 portant application, dans les ministères économiques et financiers, de l'article 7 du décret n°2016-151 du 11 février 2016 relatif aux conditions et modalités de mise en œuvre du télétravail dans la fonction publique et la magistrature, le télétravailleur bénéficie des mêmes droits et est soumis aux mêmes obligations que les agents travaillant sur site, tels que décrits dans la présente charte.

PSL met à la disposition de l'utilisateur ou l'utilisatrice le matériel lui permettant d'exercer son activité professionnelle à son domicile et en assure la maintenance. Les équipements fournis restent la propriété de PSL. Ils devront être restitué par l'usager en cas de départ de PSL ou obsolescence. Le télétravailleur ou la télétravailleuse ne peut utiliser un autre matériel que celui fourni par PSL. Il ou elle s'engage à réserver l'usage des équipements mis à disposition par PSL à un usage strictement professionnel et à prendre soin de l'équipement qui lui est confié tel que mentionné dans les précédents articles.

Les règles relatives à la sécurité des systèmes d'information et de protection des données pour l'utilisateur ou l'utilisatrice en fonction sur site s'appliquent au télétravailleur ou la télétravailleuse. Ainsi, celui-ci ou celle-ci doit se conformer aux règles relatives à la sécurité des systèmes d'information et veiller à l'intégrité et à la bonne conservation des données auxquelles il ou elle a accès dans le cadre professionnel.

Il ou elle informe sans délai leur responsable hiérarchique ainsi que le RA ou le RSSI en cas de panne, de mauvais fonctionnement, de détérioration, de perte ou de vol du matériel mis à disposition.

TITRE IV – DISPOSITIONS FINALES

Article 20 – Sanction du non-respect des dispositions de la charte

En cas de non-respect des dispositions de la présente charte, PSL peut prendre toutes mesures conservatoires s'imposant à l'encontre d'un utilisateur ou d'une utilisatrice, notamment, la récupération du matériel, le retrait des données de connexion, sans préjudice d'éventuelles procédures disciplinaires ou pénales qui seraient engagées.

ARTICLE 21– Entrée en vigueur

La présente charte a été validée par les conseils de PSL, elle est applicable à compter de son approbation par le conseil d'administration de l'Université du 26 juin 2025 à tous les utilisateurs et utilisatrices qui devront prendre en compte les articles de la charte, à partir de la date citée à cet article
Ce document annule et remplace tous les précédents documents de même nature émis par PSL relatifs à l'utilisation des SI.

ANNEXE A – RESTRICTION D'UTILISATION D'INTERNET

Charte relative à l'usage du système d'information et des technologies de l'information et de la communication à PSL

Objet	Public	Limite	Description
Restriction navigation	Tous	Risque pénal (*)	• Pornographie condamnée en droit français • Drogues • Musiques, Films, Logiciels Piratés • Peer to peer • Terrorisme - Incitation à la Violence – Explosifs et poisons • Racisme - Discrimination - Révisionnisme • Armes • Immigration clandestine et travail illégal • Alcool et tabac condamnés par la loi française • Vente de médicaments condamnée par la loi française • Contrefaçon • Piratage • Jeux d'argent et Casinos condamnés par la loi française
Restriction navigation	Tous	Risque de sécurité (*)	• Virus - Spyware - Phishing - Codes malicieux • Domaines Parkés • Proxy - Cache - Redirecteur

ANNEXE B – UTILISATION DES DONNEES PERSONNELLES DES PERSONNELS

Conformément à l'article 12, 13 et 14 du règlement général pour la protection des données (RGPD) PSL est tenu à une obligation de transparence vis-à-vis de ses employés. La présente annexe a pour objet de récapituler les finalités de traitement ainsi que les types de données récoltées dans le cadre de la gestion de ses ressources humaines.

INFORMATIONS SUR LE TRAITEMENT DE DONNEES	
1. RESPONSABLE DE TRAITEMENT	Le responsable de traitement est l'employeur du salarié, alternativement : - La fondation « Paris sciences et lettres » ; - L'Université « Paris sciences et lettres ». Sises 60 rue Mazarine 75006 Paris. Représentées par leur Président, M. El Mouhoub MOUHOUD.
2. FINALITES DU TRAITEMENT	Le traitement opéré par PSL a pour objet d'assurer les fonctions de base de la gestion administrative de ses personnels.
3. SOUS-FINALITES DU TRAITEMENT	La gestion administrative recouvre cumulativement la gestion : - Du dossier personnel individuel de chaque personnel ; - Des outils informatiques nécessaires à l'exercice de leurs fonctions ; - De leur rémunération et des différentes déclarations et paiement des cotisations sociales afférentes ; - De leur évaluation professionnelle ; - Du suivi de leur carrière ; - Des formations professionnelles ; - Le cas échéant, de l'organisation des élections professionnelles et des instances représentatives du personnel.
4. BASE LEGALE DU TRAITEMENT	Le traitement est fondé sur les obligations légales de PSL en tant qu'employeur tant vis-à-vis de ses salariés de droit privé que de ses agents publics. .
5. TYPES DE DONNEES TRAITEES	- Les données *d'identité :* nom, prénom, civilité, date de naissance, nationalité, département de naissance, adresse administrative, photographie, le cas échéant, le permis de travail ; - La situation *familiale* du salarié : marié, pacsé, concubinage, enfants à charge, coordonnées des personnes à prévenir en cas d'urgence ; - La situation *professionnelle* du salarié : niveau d'études, photocopies des diplômes ; - Les éléments financiers et de protection sociale : numéro de sécurité sociale, le relevé d'identité bancaire (RIB), photocopie de la carte vitale.
6. TRANSFERT EXTERNE	Oui : en cas d'obligation légale vis-à-vis des administrations publiques (caisse primaire d'assurance maladie, ministère du travail…).
7. TRANSFERT HORS DE L'UNION EUROPEENNE	Non
8. DUREE DE CONSERVATION DES DONNEES	Le dossier de l'agent contenant ses informations personnelles sont conservées pour dix années qui suivent sa sortie des effectifs de PSL. Il sera ensuite définitivement supprimé, sous réserves d'éventuelles obligations réglementaires.

ANNEXE C – UTILISATION DES DONNEES PERSONNELLES DES ETUDIANTS ET ETUDIANTES

Conformément à l'article 12, 13 et 14 du règlement général pour la protection des données (RGPD) PSL est tenu à une obligation de transparence vis-à-vis de ses étudiants et étudiantes La présente annexe a pour objet de récapituler les finalités de traitement ainsi que les types de données récoltées dans le cadre de la gestion de la scolarité.

INFORMATIONS SUR LE TRAITEMENT DE DONNEES	
1. RESPONSABLE DE TRAITEMENT	Le responsable de traitement est l'Université « Paris sciences et lettres ». Sises 60 rue Mazarine 75006 Paris. Représentées par leur Président, M. El Mouhoub MOUHOUD.
2. FINALITES DU TRAITEMENT	Le traitement opéré par PSL a pour objet d'assurer la gestion administrative et pédagogique des étudiants, pour les diplômes directement opérés par elle. Le traitement a aussi pour objet de permettre la réalisation d'enquêtes concernant le parcours professionnel des anciens étudiants après l'obtention de leur diplôme
3. SOUS-FINALITES DU TRAITEMENT	La gestion administrative recouvre cumulativement la gestion : - Les inscriptions administratives et pédagogiques ; - De l'emploi du temps et de l'assiduité ; - Des relevés de notes ; - De l'obtention de leur diplôme ; - Des stages, projets de césure…
4. BASE LEGALE DU TRAITEMENT	Mission d'intérêt public exercée par l'Université PSL
5. TYPES DE DONNEES TRAITEES	Les données sont collectées au moment de l'inscription de l'étudiant et comprennent : - Les données *d'identité :* nom, prénom, civilité, date de naissance, nationalité, département de naissance, adresse administrative, photographie d'identité, adresse mail personnelle ou institutionnelle numéro de téléphone ; - La situation *familiale* : responsables légaux le cas échéant ; - La situation scolaire : relevé de notes, établissements précédents, diplômes, stages ; - La situation *économique* : situation boursière et échelon, attestation CVEC ;
6. TRANSFERT EXTERNE	Oui : en cas d'obligation légale, certaines données pourront être remontées notamment au ministère de tutelle, au rectorat de Paris, au Crous, à la Cité internationale universitaire de Paris ou encore vers ses établissements-composantes.
7. TRANSFERT HORS DE L'UNION EUROPEENNE	Non
8. DUREE DE CONSERVATION DES DONNEES	Le dossier de l'étudiant est conservé durant 10 ans à compter de l'obtention de son diplôme (ou à défaut de son départ de l'établissement). Il sera ensuite définitivement supprimé, à l'exception des éventuels documents présentant un intérêt archivistique certain et qui seront archivés dans les conditions de l'article L211-1 et suivants du Code du patrimoine.