

ANNEXE 1 AU REGLEMENT INTERIEUR D'UNIVERSITE PARIS CITE

Charte d'usage des Systèmes d'Information d'Université Paris Cité

I.	Objet et champ d'application	2
	a. Personnes concernées	2
	b. Systèmes d'information	2
	c. Usages concernés	2
II.	Principes d'usage	3
	a. Utilisation conforme aux lois et règlements en vigueur.....	3
	b. Usage général.....	3
	i. Usage professionnel ou étudiant	3
	ii. Usage à titre privé.....	4
	iii. Conditions d'accès et authentification	4
	c. Usage spécifique.....	4
	i. Mobilité et accès distant.....	4
	ii. Télétravail	4
	iii. Utilisation des outils informatiques par les organisations syndicales.....	5
	iv. Unités mixtes de recherche et spécificité défense	5
	d. Configuration du poste de travail	5
	e. Gestion des Média USB	6
	f. Messagerie électronique	6
	g. Téléphonie fixe et mobile.....	7
	h. Internet et intranet.....	7
	i. Gestion des absences et des départs.....	7
	j. Bonnes pratiques	8
III.	Protection de la propriété intellectuelle, des informations et des données	8
	a. Propriété intellectuelle, droit à l'image	8
	b. Secret et confidentialité.....	9
	c. Protection des données à caractère personnel	9
	i. Registre des activités de traitement et transparence sur les traitements	10
	ii. Finalité des données personnelles collectées	10
	iii. Confidentialité des données personnelles	10
	iv. Durée de conservation des données	10
IV.	Règles de sécurité	11
	a. Devoirs de signalement et d'information	12
V.	Mesures de contrôle	13
	a. Administration des systèmes d'information	13
	b. Les systèmes automatiques de filtrage	13
	c. Les systèmes automatiques de traçabilité	13
VI.	Sanctions	14
VII.	Glossaire des termes clés	14
VIII.	Modalités d'entrée en vigueur de la charte	15



I. Objet et champ d'application

Université Paris Cité, ci-après dénommée « l'Université », accorde la plus grande importance :

- à la confidentialité et à la sécurité de l'ensemble des informations et des données personnelles collectées et traitées dans le cadre de ses activités, notamment au regard de ses missions de service public ;
- à la sécurité des moyens informatiques, réseaux, télécommunication (fixes et mobiles) et reprographiques, de traitement et de stockage de l'information et à l'usage qui en est fait au sein de ses services ;
- au respect des obligations légales en matière de protection des données à caractère personnel et de sécurité des systèmes d'information ;
- au respect des obligations légales en matière de droit de l'information, notamment sous l'angle de la propriété intellectuelle.

L'objectif de la présente charte est de conduire chacun à être acteur des usages et de la sécurité des Systèmes d'information (VII.a) de l'Université.

La présente charte définit les règles générales d'utilisation des systèmes d'information de l'Université conformément au cadre légal et réglementaire en vigueur que l'Utilisateur (VII.b) et l'Université s'engagent à respecter, elle précise les droits et devoirs de chacun. Elle tient compte notamment des recommandations de la Commission nationale de l'informatique et des libertés (CNIL) et de celles de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), ainsi que des dispositions de la charte du réseau RENATER.

Elle vise également à informer les Utilisateurs des mesures de contrôle des Systèmes d'information mis en œuvre par l'Université afin d'en assurer la sécurité et la bonne administration.

La présente charte, annexée au Règlement intérieur de l'Université, est portée à la connaissance de tout Utilisateur des systèmes d'information d'Université Paris Cité. Elle est applicable de fait et produit, à ce titre, les mêmes effets.

Pour une meilleure compréhension de la charte, l'Utilisateur est invité à contacter le Responsable de la sécurité des systèmes d'information (RSSI) de l'Université rsssi@u-paris.fr

a. Personnes concernées

La charte est applicable, et donc opposable, à toute personne autorisée à accéder aux systèmes d'information notamment, les personnels titulaires ou non titulaires, stagiaires, étudiants, hébergés, personnels de sociétés prestataires d'Université Paris Cité, visiteurs occasionnels, unités et laboratoires de recherche, et toute autre structure de recherche.

b. Systèmes d'information

Est visé par la charte, l'ensemble des systèmes d'information qui sont la propriété de l'Université et/ou qui sont mis à la disposition des Utilisateurs à des fins professionnelles.

c. Usages concernés

La charte s'applique aux types d'usage, de moyens et de ressources informatiques et numériques sous-mentionnés, quelle que soit leur fréquence ou leur périodicité et qu'ils aient lieu :

- dans les locaux de l'Université, quelle que soit leur localisation ;
- dans le cadre d'un accès distant, quel que soit le lieu de cet accès.

L'établissement étant raccordé au réseau national RENATER, tous les types d'usage des moyens et ressources informatiques et numériques doivent être conformes à la charte RENATER consultable sur le site de RENATER



<https://www.renater.fr>

II. Principes d'usage

a. Utilisation conforme aux lois et règlements en vigueur

Respect de la propriété intellectuelle

Université Paris Cité rappelle que l'utilisation des moyens 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, notamment :

- les droits acquittés par l'Université pour permettre l'accès à des contenus numériques sous droits couvrent l'accès à ces ressources hors l'enceinte de l'établissement pour les seuls étudiants et personnels d'Université Paris Cité. L'usage de ces ressources par tout autre Utilisateur est limité à la consultation sur les postes informatiques situés dans l'emprise de l'établissement ;
- il est formellement interdit de copier, même pour son usage privé, l'intégralité ou une partie substantielle des contenus numériques sous droits mis à la disposition de ses Utilisateurs par Université Paris Cité, sous réserve du droit des tiers et de l'application de la législation nationale et européenne en vigueur ;
- il est formellement interdit de diffuser à un tiers, même gratuitement, quelque contenu protégé que ce soit mis à la disposition de ses étudiants et personnels par Université Paris Cité.

Respect de la vie privée

Le droit à la vie privée, le droit à l'image, issus de l'article 9 du code civil, ainsi que le droit de représentation impliquent qu'aucune image ou information relative à la vie privée d'autrui ne doit être mise en ligne sans le consentement de la personne intéressée.

Responsabilité en matière de communication en ligne et transmission d'informations à un tiers

L'Utilisateur devra entre autres s'abstenir :

- de diffuser des messages diffamatoires ou injurieux (ces faits sont pénalement et/ou disciplinairement répréhensibles quel que soit leur mode de diffusion, public ou privé) ;
- d'utiliser certaines formes d'apologie (crime, racisme, négationnisme, crimes de guerre, ...) ;
- d'utiliser toute forme de provocation à la haine raciale ;
- de diffuser des informations confidentielles sans autorisation préalable d'une personne habilitée.

L'utilisation des Systèmes d'information (notamment les logiciels, applications, services et contenus numériques) mis à la disposition de l'Utilisateur par Université Paris Cité, est conditionnée au respect et à la mise en œuvre des Conditions générales d'utilisation, Guide d'usage ou Charte d'utilisation encadrant leur usage et figurant sur une page dédiée, accessible à tout Utilisateur.

b. Usage général

Chaque Utilisateur accède aux ressources numériques nécessaires à l'exercice de son activité professionnelle ou étudiante dans les conditions définies par Université Paris Cité.

i. Usage professionnel ou étudiant

Les dispositifs de communications électroniques (utilisation des ressources informatiques, usage des services Internet, usage du réseau) sont mis à disposition des Utilisateurs pour l'exercice de leur activité professionnelle ou étudiante au sein d'Université Paris Cité. Cet usage ne doit pas être contraire à la loi, l'ordre public et ne doit pas mettre en cause l'intérêt et la réputation de l'établissement.

L'activité professionnelle doit être notamment entendue comme celle définie par les textes spécifiant les missions du service public de l'enseignement supérieur, à savoir :

- La formation initiale et continue ;
- La recherche scientifique et technologique, la diffusion et la valorisation de ses résultats ;
- L'orientation et l'insertion professionnelle ;
- La diffusion de la culture et l'information scientifique et technique ;
- La participation à la construction de l'Espace européen de l'enseignement supérieur et de la



- recherche;
- La coopération internationale.

ii. Usage à titre privé

L'utilisation à titre privé des Systèmes d'information et de communication est tolérée, mais doit être raisonnable, non lucrative, loyale et conforme aux règles et lois en vigueur. Elle ne doit pas nuire à la qualité du travail de l'Utilisateur, au temps qu'il y consacre et au bon fonctionnement du service.

En toute hypothèse, le surcoût qui résulte de l'utilisation privée résiduelle des Systèmes d'information doit demeurer négligeable au regard du coût global d'exploitation.

Toute information est réputée professionnelle à l'exclusion des données explicitement désignées par l'Utilisateur comme relevant de sa vie privée. Ainsi, il appartient à l'Utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu explicitement à cet effet en mentionnant le caractère privé sur la ressource. L'Utilisateur devra ainsi conserver ses informations privées dans un dossier intitulé « privé ». Ce dossier peut éventuellement être consulté par la DSIN dans le cadre d'une remédiation à la suite d'une crise produite par une cyberattaque (cf. Politiques de Sécurité du Système d'Information).

Les espaces de stockages intitulés « Mes documents », « perso », « personnel » ou identifiés par les initiales de l'Utilisateur sont réputés contenir des données professionnelles.

L'Utilisateur ne doit pas transformer la totalité de l'espace de stockage mis à sa disposition par Université Paris Cité en un espace intitulé « privé », l'usage privé doit rester marginal.

Le dossier intitulé « privé » doit être placé à la racine de son espace de stockage (lecteur partagé/réseau ou au premier niveau dans le répertoire « Mes documents » sous windows).

La sauvegarde régulière des données à caractère privé incombe à l'Utilisateur.

iii. Conditions d'accès et authentification

L'accès aux ressources numériques repose sur l'utilisation d'un « compte UP » fourni à l'Utilisateur lors de son arrivée à Université Paris Cité. Un mot de passe défini par l'Utilisateur est associé à ce compte. La « robustesse » de ce mot de passe contrainte par un outil mis à disposition par l'établissement est de la responsabilité de l'Utilisateur.

Les moyens d'authentification sont personnels, confidentiels et incessibles.

c. Usage spécifique

i. Mobilité et accès distant

Dans le cadre de ses déplacements professionnels, quelle que soit leur durée ou leur fréquence, l'Utilisateur assure la garde et la responsabilité des données et des outils du système d'information de l'établissement qu'il utilise.

Il se doit d'adopter une attitude responsable au regard des informations, données et ressources des systèmes d'information de l'établissement qu'il pourrait être amené à manipuler ou à échanger. En cas d'incident avéré ou de doute, l'Utilisateur doit immédiatement en aviser le RSSI de l'Université rss@u-paris.fr.

ii. Télétravail

L'Université se réserve la possibilité de mettre en œuvre du télétravail selon la législation en vigueur. Le cas échéant, l'utilisation autorisée au télétravail devra suivre les dispositions de la charte ainsi que l'ensemble des procédures et instructions données par l'Université pour l'utilisation des systèmes d'information.

Dans le cadre de cette mise en œuvre, Université Paris Cité met à disposition des télétravailleurs les équipements en matériels informatiques, ordinateurs portables et logiciels nécessaires à l'exercice de leur activité professionnelle. L'équipement sera fourni et maintenu par Université Paris Cité et restera sa propriété.

Ces matériels informatiques sont réservés à un usage exclusivement professionnel et seul l'agent de l'université en a donc l'usage. L'utilisation par un autre membre de la cellule familiale est formellement interdite. Par ailleurs, les données du poste sont professionnelles et ne doivent pas être partagées avec les membres du foyer.



Les télétravailleurs doivent disposer sur le lieu de télétravail d'une connexion internet afin d'accéder aux systèmes d'information d'Université Paris Cité. En cas de problème avec leur connexion internet, les télétravailleurs devront contacter leur fournisseur d'accès. Il est par ailleurs interdit de se connecter à internet sur un réseau public (Wifi public, hotspot, ou accès de type portail d'authentification).

Afin d'assurer la sécurité des communications et des données, les télétravailleurs ne doivent pas installer de logiciels non autorisés par la Direction des Systèmes d'Information et du Numérique. Les télétravailleurs ne devront accéder aux systèmes d'information d'Université Paris Cité qu'après avoir établi une connexion sécurisée en activant le VPN (réseau privé virtuel) installé sur leur poste de travail.

Le droit à la déconnexion

Le droit à la déconnexion vise à respecter le temps de repos et de congés des personnels d'Université Paris Cité ainsi que leur vie personnelle et familiale.

Il limite les connexions aux heures de travail en fonction de l'activité et des astreintes du personnel. Les personnels ne sont pas tenus d'être connectés en dehors de leurs horaires de travail.

iii. Utilisation des outils informatiques par les organisations syndicales

Les organisations syndicales représentatives utilisent les outils informatiques qui leur sont attribués pour l'exercice de leur mandat syndical. L'utilisation de ces outils se fait sans contrôle des données, à l'exception du paramétrage initial desdits outils ou à une intervention dans le cas d'une crise cyber (lecture des logs et journaux des applications et des postes de travail notamment. Exemple : log des antivirus) conformément à la Politique de Sécurité des Systèmes d'Information.

Ils disposent d'une adresse électronique dédiée (organisation.**syndicale@u-paris.fr**). Ces adresses électroniques seront seules habilitées à transmettre une communication d'origine syndicale et à utiliser les listes de diffusion mises à dispositions par l'administration.

Il est rappelé que toute communication entre les agents et les organisations syndicales sont individuelles et confidentielles. Sous réserve des conditions générales de sécurité des systèmes d'information, les messages transmis ou émis à ces adresses mails se font sans blocage et sans lecture par un tiers.

iv. Unités mixtes de recherche et spécificité défense

Dans le cas d'une UMR, celle-ci peut prévoir des restrictions d'accès spécifiques à son organisation.

Les Utilisateurs de ces unités sont notamment soumis au respect, quand elles existent, des Politiques de sécurité du système d'information de l'unité (PSSI) édictées par les tutelles correspondantes (Université, CNRS, INSERM, INRIA, ...).

La transmission des données classifiées de défense au sens de l'IGI 300 est interdite, sauf dispositif spécifique agréé par l'ANSSI. Par ailleurs, tout équipement traitant des données classifiées de défense doit être de même niveau que la donnée classifiée la plus haute (Secret ou Très Secret).

La transmission des données dites sensibles au sens de l'II n°901 (ie sensible pour l'organisation ou de niveau Diffusion Restreinte) doit être traitée via les moyens de chiffrement appropriés qualifiés par l'ANSSI. Des informations de niveau DR ne peuvent être traitées sur des équipements ne disposant pas de ce niveau de protection.

d. Configuration du poste de travail

Université Paris Cité met à disposition des Utilisateurs un poste de travail doté des outils informatiques nécessaires à l'accomplissement de leurs fonctions. L'Utilisateur ne doit pas :

- modifier ces équipements et leur fonctionnement, leur paramétrage, ainsi que leur configuration physique ou logicielle ;



- connecter ou déconnecter du réseau les outils informatiques et de communications sans y avoir été autorisé par l'équipe informatique interne ;
- déplacer l'équipement informatique (sauf s'il s'agit d'un « équipement nomade ») ;
- nuire au fonctionnement des outils informatiques et de communication.

e. Gestion des médias USB

Il est interdit de connecter à son poste de travail tout équipement non nécessaire à l'activité professionnelle.

A titre d'exemple sont interdits à la connexion sur le poste de travail les équipements suivants (liste non exhaustive) :

- Téléphone mobile personnel ou professionnel (ils sont vecteurs de nombreuses failles de sécurité). Il est toutefois autorisé de se servir des téléphones comme point d'accès internet via wifi ;
- Cigarettes électroniques ;
- Webcam personnelle ;
- ...

Pour les usages des supports amovibles de stockage (clés USB ou disques durs), il est recommandé de vérifier l'innocuité de ces derniers avant de connecter ces médias sur un poste de travail professionnel.

Il est interdit de connecter un de ces supports si l'origine de ce dernier n'est pas maîtrisée (ex : clé USB trouvée).

f. Messagerie électronique

(a) Conditions d'utilisation

Tout Utilisateur doit utiliser l'adresse électronique professionnelle qui lui a été attribuée à sa prise de fonction.

La messagerie mise à disposition des Utilisateurs est destinée à un usage professionnel (administration, pédagogie, recherche). L'utilisation de la messagerie à des fins personnelles est tolérée si elle n'affecte pas le travail du personnel ni la sécurité du réseau informatique d'Université Paris Cité. Toutefois, l'Université recommande plutôt l'utilisation de matériel personnel pour l'utilisation de la messagerie à des fins personnelles.

Tout message qui comportera la mention expresse de son caractère privé bénéficiera du droit au respect de la vie privée et du secret des correspondances. A défaut, le message est présumé professionnel.

Pour lui conférer un caractère privé, l'objet du message doit contenir la mention « privé » ou le message doit être déposé dans un dossier intitulé « Privé ».

Université Paris Cité s'interdit d'accéder aux dossiers et aux messages identifiés comme « privés » dans l'objet de la messagerie de l'agent.

L'utilisation de la messagerie électronique doit se conformer aux règles d'usage définies et validées par Université Paris Cité :

- volumétrie de la messagerie ;
- taille maximale de l'envoi et de la réception d'un message ;
- nombre limité de destinataires simultanés lors de l'envoi d'un message ;
- respect de la confidentialité des données (aucune donnée sensible ne doit transiter via la messagerie sans les mesures de sécurité ad hoc cf. II n°901)
- gestion de l'archivage de la messagerie.

Le transfert de messages, ainsi que leurs pièces jointes, à caractère professionnel sur des messageries personnelles est soumis aux mêmes règles que les copies de données sur supports externes.

(b) Statut et valeur juridique des messages

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles 1369.1 à 1369.11 du code civil.

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



(c) Stockage et archivage des messages

Chaque Utilisateur doit organiser et mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou utiles en tant qu'éléments de preuve, conformément aux règles édictées par le Département des Archives de l'établissement.

À ce titre, il doit notamment se conformer aux règles définies dans la présente charte et, le cas échéant, dans le ou les guides d'utilisation établi(s) par le service ou par l'établissement.

g. Téléphonie fixe et mobile

Université Paris Cité met à disposition des Utilisateurs, pour l'exercice de leur activité professionnelle, des téléphones fixes et mobiles.

L'utilisation du téléphone à titre privé est admise à condition qu'elle demeure marginale.

Des restrictions d'utilisation par les personnels d'Université Paris Cité des téléphones fixes et mobiles peuvent être mises en place en tenant compte de leurs missions.

A titre d'exemple, certains postes sont limités aux appels nationaux, d'autres peuvent passer des appels internationaux.

Université Paris Cité s'interdit de mettre en œuvre un suivi individuel de l'utilisation des services de télécommunications. Seules des statistiques globales sont réalisées sur l'ensemble des appels entrants et sortants. Elle vérifie que les consommations n'excèdent pas les limites des contrats passés avec les opérateurs.

Université Paris Cité s'interdit d'accéder à l'intégralité des numéros appelés *via* l'autocommutateur mis en place et *via* les téléphones mobiles. Toutefois, en cas d'utilisation manifestement anormale, la DSIN, sur demande du Directeur général des services, se réserve le droit d'accéder aux numéros complets des relevés individuels.

h. Internet et Intranet

Les Utilisateurs peuvent consulter les sites Internet présentant un lien direct et nécessaire avec l'activité professionnelle, de quelque nature qu'ils soient.

Toutefois, une utilisation ponctuelle et marginale, pour un motif personnel, des sites Internet dont le contenu n'est pas contraire à la loi, l'ordre public, et ne met pas en cause l'intérêt et la réputation de l'établissement, est admise.

(a) Publications sur les sites Internet et Intranet d'Université Paris Cité

Toute publication de pages professionnelles (*VII.e*) sur les sites Internet ou Intranet de l'Université, ou sur ses comptes institutionnels sur les réseaux sociaux, doit être validée par un responsable de site ou responsable de publication nommément désigné, sous réserve des libertés des universitaires.

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

(b) Téléchargements

Tout téléchargement de fichiers, notamment de sons ou d'images, sur le réseau Internet doit s'effectuer dans le respect des droits de la propriété intellectuelle. Université Paris Cité se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information (virus susceptibles d'altérer le bon fonctionnement des Systèmes d'information d'Université Paris Cité, code malicieux, programmes espions ...).

À l'inverse, l'utilisation du réseau pour l'offre d'un service disponible depuis l'Internet doit être rationnelle de manière à éviter toute consommation abusive ou pénalisante. L'offre de sons, d'images, de vidéos, de logiciels et tous autres documents doivent s'effectuer dans le respect des droits de la propriété intellectuelle et être en rapport avec les missions d'enseignement et de recherche d'Université Paris Cité.

i. Gestion des absences et des départs



En cas d'absence prolongée pour quelque raison et durée que ce soit, ou de départ de l'Utilisateur, l'Université se réserve le droit :

- de mettre en place une solution raisonnée de contrôle des messages électroniques ou toute autre solution technique permettant d'assurer la continuité de service (exemple : accès à la boîte mail de l'individu par le supérieur hiérarchique en accord avec la protection des données personnelles) ;
- d'accéder directement aux différents dossiers, répertoires, courriers électroniques et plus généralement tout document à caractère professionnel de l'Utilisateur en cas d'incident de sécurité ou lorsque l'activité est mise en péril et sur décision de la présidence ou du DGS et du Fonctionnaire Sécurité Défense. L'utilisateur sera informé par la voie hiérarchique dans un délai de 48h si tel était le cas.

En cas de départ :

- l'Utilisateur doit lors de son départ définitif du service ou de l'établissement, détruire son espace de données à caractère privé, la responsabilité de l'Université ne pouvant être engagée quant à la conservation de cet espace. Dans le cas où cet espace de données à caractère privé n'aurait pas été détruit par l'Utilisateur, l'Université s'engage à ne divulguer à des tiers aucun des éléments y figurant, sauf cas prévus par la réglementation et cela jusqu'à effacement pour réattribution du matériel ;
- l'Utilisateur doit organiser la bonne transmission à son successeur des données professionnelles utiles à la bonne continuité du service public : la destruction de tout ou partie de ces données constitue une faute professionnelle, susceptible, au-delà des sanctions disciplinaires, de poursuites pénales en fonction du préjudice causé à l'Université ;
- l'Utilisateur doit restituer au service informatique interne les matériels mis à sa disposition par l'Université ;
- tous les accès de l'Utilisateur seront désactivés et il sera désabonné de toutes les listes de diffusion auxquelles il s'était abonné ou a été abonné par autrui. Et ce, pour garantir la continuité de service, à l'expiration du sursis accordé par l'Université au regard des fonctions qu'il exerçait ;
- concernant son compte de messagerie professionnelle, l'Utilisateur s'engage à paramétrer un message automatique d'absence indiquant, s'il en a connaissance, les coordonnées de son remplaçant ou, à défaut, celui de son supérieur hiérarchique. Le compte de messagerie professionnel ainsi que les données y figurant seront supprimés à l'issue d'un délai de 3 mois après le départ de l'agent sauf dérogation accordée par le DGS.

j. Bonnes pratiques

Messagerie électronique

(a) Contenu des messages électroniques

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place : dans ce cas, les termes en sont précisés dans un guide d'utilisation de la messagerie qui est porté à la connaissance des Utilisateurs.

(b) Émission et réception des messages

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.

(c) Courriel non sollicité

Université Paris Cité dispose d'un outil permettant de lutter contre la propagation des messages non désirés (spam). Aussi, afin de ne pas accentuer davantage l'encombrement du réseau lié à ce phénomène, les Utilisateurs sont invités à limiter leur consentement explicite préalable à recevoir un message de type commercial, newsletter, abonnements ou autres, et de ne s'abonner qu'à un nombre limité de listes de diffusion notamment si elles ne relèvent pas du cadre strictement professionnel.

III. Protection de la propriété intellectuelle, des informations et des données

a. Propriété intellectuelle, droit à l'image



L'utilisation des systèmes d'information de l'Université implique le respect des droits de propriété intellectuelle et du droit à l'image.

Sans que cette liste soit exhaustive, l'Utilisateur s'engage à :

- utiliser les logiciels et applications, dans les conditions de la licence souscrite par l'Université ;
- ne pas effectuer de copie illicite de logiciel ou d'applications et, *a fortiori*, de tenter d'installer des logiciels ou applications pour lesquels l'Université ne posséderait pas un droit d'usage ;
- ne pas reproduire, copier, utiliser remettre à des tiers ou diffuser, les bases de données, pages web, dessins, modèles, logos ou autres créations de l'Université ou de tiers protégés par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation du titulaire de ces droits ;
- ne pas reproduire, copier ou diffuser des textes, des images, des photographies, des œuvres musicales, audiovisuelles ou multimédia et, plus généralement, toute création ou invention provenant du réseau internet, d'applications web ou mobiles, sans autorisation ou licence ;
- ne pas reproduire, copier, utiliser ou diffuser des éléments susceptibles de porter atteinte à l'image ou à la vie privée des Utilisateurs ou de tiers à l'Université.

b. Secret et confidentialité

La sauvegarde des intérêts de l'Université nécessite le respect par l'Utilisateur d'une obligation générale et permanente de confidentialité, de discrétion et de secret professionnel à l'égard des informations et des données dont il a connaissance dans le cadre de l'exercice de son activité professionnelle.

Le respect de cette obligation implique notamment de :

- veiller à ce que les tiers non autorisés n'aient pas connaissance de telles informations et données ;
- n'accéder qu'aux informations et données en rapport direct avec sa fonction et ne pas chercher, en conséquence, à prendre connaissance d'informations réservées à d'autres Utilisateurs ;
- ne pas extraire ces informations et données confidentielles et ne pas les reproduire sans l'accord préalable du supérieur hiérarchique et/ou les détourner de leur utilisation normale à des fins non professionnelles ;
- d'une manière générale, respecter les règles d'éthique professionnelle, de déontologie, ainsi que les obligations de réserve et devoir de discrétion conformes à la loi Le Pors (n°83-634), qui fixe les droits et obligations des agents publics.

La diffusion de toute information ou donnée confidentielle ne peut être réalisée qu'aux conditions suivantes :

- habilitation de l'émetteur ;
- désignation d'un destinataire autorisé ;
- respect d'une procédure sécurisée.

c. Protection des données à caractère personnel

Université Paris Cité accorde une importance toute particulière à la protection des données à caractère personnel (VII.c) des Utilisateurs de ses ressources informatiques et numériques. En tant que responsable de traitement, Université Paris Cité est soumise au respect des dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après le « RGPD ») ainsi qu'à celles de la loi « Informatique et Libertés » (loi n° 78-17 du 6 janvier 1978 modifiée). Ces textes définissent les conditions dans lesquelles les traitements de données à caractère personnel peuvent être effectués.

Université Paris Cité a désigné un Délégué à la protection des données à caractère personnel (DPD). Ce dernier a pour mission de veiller au respect des dispositions du RGPD et de la loi n°78-17 du 6 janvier 1978 modifiée, au sein de l'Université.

Le Délégué à la protection des données est obligatoirement informé et consulté par les services de l'Université préalablement à la création de tout traitement de données à caractère personnel afin de les accompagner dans leur mise en œuvre conformément à la réglementation.

Le Délégué à la protection des données recense dans un registre la liste de l'ensemble des traitements de données à caractère personnel d'Université Paris Cité.

Chaque Utilisateur dispose d'un droit d'accès, de rectification, d'effacement, de portabilité, à la limitation du



traitement et d'un droit d'opposition, sur les données le concernant. Ces droits s'exercent auprès du responsable du traitement dans le cadre des limites prévues par la loi.

Le DPD veille au respect des droits des personnes concernées sur leurs données. En cas de difficultés rencontrées lors de l'exercice de ces droits, les personnes concernées peuvent saisir le Délégué à la protection des données à l'adresse électronique dpo@u-paris.fr ou par courrier, à l'adresse postale suivante :

Le Délégué à la protection des données personnelles d'Université Paris Cité
Direction générale déléguée aux affaires juridiques
85 boulevard Saint-germain
75006 Paris

i. Registre des activités de traitement et transparence sur les traitements

L'Université s'engage à ce que les traitements de données personnelles soient mis en œuvre conformément à la réglementation en vigueur.

Ainsi, tout traitement de données personnelles doit être inscrit au registre des activités de traitement d'Université Paris Cité.

Préalablement à la mise en œuvre de tout traitement de données personnelles, les personnes concernées sont informées :

- du responsable du traitement et des objectifs du recueil de ces données (finalités)
- de la base juridique du traitement de données personnelles ;
- du caractère obligatoire ou facultatif du recueil des données personnelles et de la liste des catégories de données traitées ;
- des catégories de personnes concernées ;
- des destinataires des données ;
- de la durée de conservation des données ;
- des mesures de sécurité (description générale) ;
- de l'existence éventuelle de transferts de données hors de l'Union européenne ou de prises de décision automatisées ;
- de leurs droits Informatique et Libertés et de la façon de les exercer auprès de l'Université.

Ces informations doivent apparaître sur tout support de collecte de données personnelles (formulaires, etc.).

ii. Finalité des données personnelles collectées

Conformément aux principes de minimisation et de proportionnalité, Université Paris Cité s'engage à ne traiter que les données adéquates, pertinentes et strictement nécessaires à la finalité du traitement. L'Université s'engage à ne pas traiter les données pour d'autres finalités que la finalité initiale, sauf à en informer la personne concernée et à recueillir son consentement préalable à la nouvelle finalité.

iii. Confidentialité des données personnelles

L'Université s'assure que seules les personnes ayant besoin d'en connaître ont accès aux données personnelles des Utilisateurs.

Toutes les personnes ayant accès aux données personnelles sont liées par un devoir de confidentialité et s'exposent à des mesures disciplinaires et/ou sanctions pénales si elles ne respectent pas ces obligations.

Toutefois, il conviendra de noter que les données peuvent être divulguées à des tiers autorisés en application d'une loi, d'un règlement ou en vertu d'une décision d'une autorité réglementaire ou judiciaire compétente.

iv. Durée de conservation des données

Les données sont stockées et conservées pour la durée nécessaire à la réalisation de la ou des



finalité(s) visée(s) et conformément aux réglementations en vigueur applicables.

IV. Règles de sécurité

Université Paris Cité met en œuvre les mécanismes de protection appropriés sur les Systèmes d'information mis à la disposition des Utilisateurs.

En particulier, tout Utilisateur des Systèmes d'information d'Université Paris Cité doit être référencé dans les Systèmes d'information de l'Université et avoir obtenu des « codes d'accès », c'est-à-dire "identifiant de connexion et mot de passe associé", qui lui sont personnels et confidentiels.

L'Utilisateur est informé que les codes d'accès constituent une mesure de sécurité permettant de protéger les données et les outils auxquels il a accès de toute utilisation malveillante ou abusive. Cette mesure ne confère pas pour autant un caractère personnel à ces données ou outils.

L'Utilisateur est responsable de l'utilisation qui est faite de ses codes d'accès, leur divulgation volontaire à un tiers engage sa responsabilité pénale et civile.

Les niveaux d'accès ouverts à l'Utilisateur sont définis en fonction de la mission qui lui est conférée. La sécurité des Systèmes d'information mis à sa disposition lui impose :

- de respecter les consignes de sécurité, notamment les règles relatives à la gestion des mots de passe ;
- de garder strictement confidentiel(s) son (ou ses) mot(s) de passe et ne pas le(s) dévoiler à un tiers ;
- de respecter la gestion des accès, en particulier ne pas utiliser les noms et mots de passe d'un autre Utilisateur, ni chercher à les connaître ;
- de protéger son certificat électronique (s'il en dispose) par un mot de passe sûr gardé secret.

L'Utilisateur s'engage à n'autoriser personne à faire usage d'un certificat électronique à sa place.

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

(a) De la part d'Université Paris Cité :

- 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 ;
- Ne pas autoriser les redirections de messagerie pour les adresses de fonctions dans la mesure où le Système d'information est accessible (après authentification) tant du réseau de l'Université que de l'extérieur.

(b) De la part de l'Utilisateur :

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

- Signaler à la DSIN (rssi@u-paris.fr) toute violation ou tentative de violation suspectée de son compte Utilisateur et de manière générale tout dysfonctionnement ;
- Ne jamais confier son identifiant/mot de passe à un tiers ;
- Ne jamais demander son identifiant/mot de passe à un collègue ou à un collaborateur ;
- Ne pas masquer sa véritable identité ;
- Ne pas usurper l'identité d'autrui ;
- Ne pas modifier et/ou contourner les paramètres de sécurité du poste de travail ;
- Ne pas copier, modifier, détruire les logiciels propriétés d'Université Paris Cité ;
- Verrouiller son ordinateur dès qu'il quitte son poste de travail ;
- Ne pas accéder à, tenter d'accéder à, supprimer ou modifier des informations qui ne lui appartiennent pas ;
- Ne pas publier sur Internet ou Intranet des informations pouvant nuire aux personnels, aux étudiants ou à l'Université ;
- Veiller aux réglementations en vigueur visant à engager les Utilisateurs sur ce qu'ils publient avec le label de l'Université ;
- Toute copie de données appartenant à Université Paris Cité sur un support externe est soumise à l'accord du



supérieur hiérarchique et doit respecter les règles définies par Université Paris Cité ;

- S'interdire d'accéder ou de tenter d'accéder à des ressources du Système d'information et aux communications entre tiers pour lesquelles il n'a pas reçu d'habilitation explicite ;
- Ne pas utiliser les services qui lui sont offerts pour proposer ou rendre accessibles à des tiers des données et informations confidentielles ou contraires à la législation en vigueur ;
- Ne pas connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés par Université Paris Cité, ou ceux dont la liste a été précisée dans un guide d'utilisation établi par le service ou par l'établissement. Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Elles peuvent être retirées à tout moment. Toute autorisation prend fin lors de la cessation de l'activité professionnelle ou étudiante qui l'a justifiée ;
- Ne pas installer, télécharger ou utiliser sur le matériel connecté au réseau d'Université Paris Cité, des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, ou sans autorisation de sa hiérarchie ;
- Ne pas déposer des données sur un serveur interne ou ouvert au grand public (Free, Orange, ...) ou sur le poste de travail d'un autre Utilisateur sans y être autorisé par les responsables habilités ;
- 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 par l'introduction de logiciels parasites (virus, chevaux de Troie, bombes logiques...). Tout travail de recherche ou autre, risquant de conduire à la violation de cette règle, ne pourra être accompli qu'avec l'autorisation du responsable de la sécurité du Système d'information de l'Université et dans le strict respect des règles qui auront alors été définies ;
- Se conformer aux dispositifs mis en place par l'Université pour lutter contre les virus et les attaques par programmes informatiques ;
- Assurer la protection de ses informations et plus particulièrement celles considérées comme sensibles, y compris en utilisant différents moyens de sauvegarde individuels ou mis à sa disposition. En particulier, il ne doit pas transporter sans protection (telle qu'un chiffrement) des données sensibles sur des supports non fiables tels que ordinateurs portables, clés USB, disques externes, etc. ;
- Ne pas quitter un poste informatique en libre-service en laissant des ressources ou services accessibles. Il doit notamment procéder à la fermeture de sa session en verrouillant son ordinateur ;
- L'Utilisateur assure la garde et la responsabilité des équipements fournis par l'Université. Il doit informer la direction compétente en cas d'incident (perte, vol, dégradation) afin qu'il soit procédé aux démarches telles que la déclaration de vol ou de plainte. Il est garant de la sécurité des équipements qui lui sont remis et ne doit pas contourner la politique de sécurité mise en place sur ces mêmes équipements ;
- Quand cela est techniquement possible, les équipements nomades (VII.d) doivent faire l'objet d'une sécurisation particulière, au regard de la sensibilité des documents qu'ils peuvent stocker, notamment par chiffrement.

Quand un ordinateur portable se trouve dans le bureau de l'agent qui en a l'usage, cet ordinateur doit être physiquement attaché à l'aide de l'antivol prévu à cet effet.

L'utilisation de smartphones professionnels comporte des risques particuliers pour la confidentialité des données, notamment en cas de perte ou de vol de ces équipements. Quand ces appareils ne sont pas utilisés pendant quelques secondes, ils doivent donc être verrouillés par un moyen adapté de manière à prévenir tout accès non autorisé aux données qu'ils contiennent.

Les intervenants extérieurs doivent s'engager à faire respecter la présente charte par leurs propres salariés et éventuelles entreprises sous-traitantes. Dès lors, les contrats signés entre Université Paris Cité et tout tiers ayant accès aux données, aux programmes informatiques ou autres moyens, doivent comporter une clause rappelant cette obligation.

a. Devoirs de signalement et d'information

Université Paris Cité doit porter à la connaissance de l'Utilisateur tout élément susceptible de lui permettre d'apprécier le niveau de risque encouru dans l'utilisation du Système d'information.

L'Utilisateur doit avertir sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté ou de toute



anomalie découverte telle une intrusion dans le Système d'information, etc. Il signale également au Responsable de la sécurité des systèmes d'information rssi@u-paris.fr toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation.

V. Mesures de contrôle

La DSIN assure le bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communication d'Université Paris Cité. Les personnels de cette direction disposent d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place.

L'Utilisateur est informé :

- que pour effectuer la maintenance corrective, curative ou évolutive, Université Paris Cité se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition ;
- que pour préserver la sécurité, l'intégrité des systèmes d'information de l'Université, la DSIN se réserve le droit d'isoler, bloquer, éteindre tout flux ou équipement qu'elle identifierait comme étant problématique (réglementation, sécurité, accès illicite,...) ;
- qu'une maintenance est précédée d'une information de l'Utilisateur sauf mesures urgentes.

Université Paris Cité informe l'Utilisateur que les Systèmes d'information et postes de travail peuvent donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus.

Les personnels en charge des opérations de contrôle ont accès à l'ensemble des données techniques. Ils sont assujettis au devoir de réserve et sont tenus de préserver la confidentialité des données qu'ils sont amenés à connaître dans le cadre de leurs fonctions.

Ils ne peuvent donc pas divulguer les informations qu'ils sont amenés à connaître dans le cadre de leur fonction dès lors que :

- ces informations sont couvertes par le secret des correspondances ou, qu'identifiées comme telles, elles relèvent de la vie privée de l'Utilisateur ;
- elles ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité ;
- elles ne tombent pas dans le champ de l'article 40 alinéa 2 du code de procédure pénale qui fait obligation à tout organe public de déférer des faits délictueux au procureur de la République.

a. Administration des systèmes d'information

Afin de surveiller le fonctionnement et de garantir la sécurité des Systèmes d'information d'Université Paris Cité, différents dispositifs sont mis en place (ex : administration à distance, centralisation des logs, ...).

Conformément au paragraphe ci-dessus, les logs des équipements (serveurs ou poste de travail notamment), ainsi que les logs applicatifs peuvent être récupérés à des fins de supervisions de sécurité (une durée de rétention sera appliquée entre 6 mois et un an en fonction des logs applicatifs concernés).

b. Les systèmes automatiques de filtrage

A titre préventif, des systèmes automatiques de filtrage permettant de diminuer les flux d'informations pour Université Paris Cité et d'assurer la sécurité et la confidentialité des données sont mis en œuvre. Il s'agit notamment du filtrage des sites Internet, de l'élimination des courriels non sollicités, du blocage de certains protocoles.

Université Paris Cité se réserve le droit de filtrer ou d'interdire l'accès à certains sites internet, de procéder au contrôle a priori ou a posteriori des sites visités et des durées d'accès correspondantes.

Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par Université Paris Cité. Des règles de sécurité spécifiques peuvent être précisées, s'il y a lieu, dans un guide d'utilisation établi par la DSIN ou l'établissement.

L'Utilisateur est informé des risques et limites inhérents à l'utilisation d'Internet par le biais d'actions de formation ou de campagnes de sensibilisation.

c. Les systèmes automatiques de traçabilité

La DSIN d'Université Paris Cité opère sans avertissement les investigations nécessaires à la résolution de



dysfonctionnements des Systèmes d'information ou de l'une de ses composantes, qui mettent en péril leur fonctionnement ou leur intégrité.

Elle s'appuie pour ce faire, sur des fichiers de journalisation (fichiers « logs ») qui recensent toutes les connexions et tentatives de connexions aux Systèmes d'information. Ces fichiers peuvent comporter les données suivantes : date, identifiant de l'Utilisateur, adresse IP et objet de l'évènement.

Les personnes habilitées au sein de la DSIN seront les seuls utilisateurs autorisés à accéder à ces informations qui sont effacées périodiquement.

VI. Sanctions

En cas de non-respect des règles définies dans la présente charte et des modalités définies dans les guides d'utilisation, la Présidente ou le Président de l'Université pourra, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des Utilisateurs, limiter les usages à titre conservatoire.

Tout abus dans l'utilisation des ressources mises à la disposition de l'Utilisateur à des fins extraprofessionnelles, est passible de sanctions.

Des sanctions en interne peuvent être prononcées, elles consistent :

- dans un premier temps, en un rappel à l'ordre émanant de la DSIN ou du service informatique de proximité, après avis de la Présidence ou de la Direction générale des services, en cas de non-respect des règles énoncées par la charte ;
- dans un second temps, et en cas de récurrence, après avis de la Présidence, de la Direction générale des services ou du supérieur hiérarchique de l'agent, en des sanctions disciplinaires adoptées après saisine de l'autorité compétente.

Le non-respect des lois et textes applicables en matière de sécurité des systèmes d'information, de protection des données personnelles et de la vie privée, et de droit de la propriété intellectuelle (contrefaçon) est pénalement répréhensible.

VII. Glossaire des termes clés

(a) Système d'information : ensemble des moyens matériels (fixes ou mobiles), logiciels, applications, services numériques, contenus en ligne, réseaux de télécommunications, mis à disposition de l'Utilisateur par Université Paris Cité. « L'informatique nomade » tels que les assistants personnels, les ordinateurs portables, les téléphones portables, etc., est également un des éléments constitutifs du Système d'information.

(b) Utilisateur : toute personne autorisée à accéder aux systèmes d'information notamment, les personnels titulaires ou non titulaires, stagiaires, étudiants, hébergés, personnels de sociétés prestataires d'Université Paris Cité, visiteurs occasionnels, unités et laboratoires de recherche, et toute autre structure de recherche.

(c) Donnée à caractère personnel ou donnée personnelle : toute information relative à une personne physique susceptible d'être identifiée ou identifiable, directement ou indirectement.

Exemples de données personnelles : nom, prénom, numéro de téléphone, adresse postale, numéro de sécurité sociale, adresse électronique, matricule interne, adresse IP, voix, photo,

L'identification d'une personne physique peut être réalisée à partir d'une seule donnée (exemple : nom) ou à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour et membre de telle association)

(d) Équipements nomades : tous les moyens techniques mobiles (ordinateur portable, imprimante portable, téléphones mobiles ou smartphones, tablettes, CD ROM, clé USB, etc.).

(e) Page Web professionnelle : page Web du domaine « u-paris.fr » (ou d'un de ses sous-domaines) placée sous la responsabilité d'un personnel de l'université, d'une association, d'un groupement ; elle doit être fiable et être obligatoirement datée, identifier son producteur et comprendre à quel titre il la rend accessible ;

Elle contient des informations de nature professionnelle, en rapport avec le métier du responsable ou avec les missions d'Université Paris Cité, ce qui implique une responsabilité sur le contenu informatif (exactitude, légalité, pertinence, ...), leur pérennité et leur intégrité ;



Elle concourt comme les autres à l'image de l'Université et des autres tutelles dans le cas des unités mixtes de recherche ; il est donc interdit d'engager abusivement l'Université et les autres tutelles ou de nuire à leur réputation ou à celle de l'un de leurs membres.

(f) logs : Dans le domaine informatique, le terme log désigne un type de fichier, ou une entité équivalente, dont la mission principale consiste à stocker un historique des événements. Diminutif de logging, le terme peut être traduit en français par "journal". Le log s'apparente ainsi à un journal de bord horodaté, qui ordonne les différents événements qui se sont produits sur un ordinateur, un serveur, etc. Il permet ainsi d'analyser heure par heure, voire minute par minute, l'activité interne d'un processus.

VIII. Modalités d'entrée en vigueur de la charte

La présente charte a été adoptée après information et consultation du Comité Social d'Administration.

Elle entrera en vigueur *un mois* à compter de sa publication par l'Université.

CONSEIL D'ADMINISTRATION

Délibération n° 2023-31

Le conseil d'administration, réuni le 22 juin 2023 à 9h30, sur convocation de la présidente par intérim d'Université Paris Cité adressée le 8 juin 2023 ;

- Vu** le code de l'éducation ;
- Vu** le décret n° 2019-209 modifié du 20 mars 2019 portant création de l'Université Paris Cité et approbation de ses statuts ;
- Vu** la délibération n° 2019-08 du conseil d'administration d'Université Paris Cité du 19 octobre 2019 relative à l'élection de madame Clarisse BERTHEZÈNE en tant que vice-présidente du conseil d'administration de l'établissement ;
- Vu** l'avis de la commission des conventions et statuts du 21 novembre 2022 ;
- Vu** l'avis du conseil social d'administration du 30 mai 2023 ;
- Vu** la délibération n° 2023-31 du sénat académique du 13 juin 2023 portant avis sur le projet de Charte Informatique d'Université Paris Cité ;
- Vu** la délibération n° 2023-26 du conseil d'administration d'Université Paris Cité du 22 juin relative à l'élection de monsieur Édouard KAMINSKI en tant que président d'Université Paris Cité.

Point de l'ordre du jour : 2.3. Charte informatique d'Université Paris Cité (vote pour approbation)

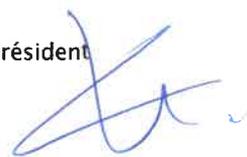
Il est demandé au conseil d'administration d'approuver la Charte informatique de l'université tel que soumise aux membres dans le dossier de séance et annexée à la présente délibération.

Après en avoir délibéré, le conseil d'administration approuve la présente délibération.

<p>Nombre de membres constituant le conseil : 28 Quorum : 14 Nombre de membres présents ou représentés : 27 Nombre de membres participant à la délibération : 27 Abstentions : 5 Votes exprimés : 22 Contre : 1 Pour : 21</p>

Fait à Paris, le **30 JUIN 2023**

Le président


Édouard KAMINSKI

En application des articles L. 410-1 à L. 412-8 du code des relations entre le public et l'administration et des articles R. 421-1 et suivants du code de justice administrative, la présente délibération pourra faire l'objet, dans un délai de deux mois à compter de sa notification et/ou de sa publication, d'un recours gracieux auprès du président d'Université Paris Cité et/ou d'un recours pour excès de pouvoir devant le Tribunal administratif de Paris.

Classé au registre des délibérations du conseil d'administration, consultable au secrétariat de la direction générale déléguée aux affaires juridiques

Affiché le :

30 JUIN 2023

Transmis au recteur le :

30 JUIN 2023