RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

UPEC
Connaissance - Action

UNIVERSITÉ PARIS-EST CRÉTEIL VAL DE MARNE

DÉLIBÉRATION

Le Conseil d'Administration de l'Université réuni en formation plénière le 13 mars 2026

DÉLIBÉRATION – CA-2026-VIE DE L'ÉTABLISSEMENT-10

RENDUE EXÉCUTOIRE LE : 30 MARS 2026

Date de transmission : 30 MARS 2026

Date de réception rectorat : 30 MARS 2026

PARIS-EST CRETEIL VAL DE MARNE - UPEC
des Affaires Juridiques et Générales
Avenue du Général de Gaulle
94010 CRETEIL Cedex
Tél. : 01.45.17.10.31

APPROUVANT LA CHARTE RELATIVE À L'USAGE DE L'INTELLIGENCE ARTIFICIELLE AU SEIN DE L'UNIVERSITÉ

VU *le Code de l'éducation ;*
VU *les statuts de l'Université Paris-Est Créteil Val-de-Marne (UPEC) approuvés par arrêté du ministre de l'éducation nationale en date du 14 novembre 1985, dans leur version issue des modifications approuvées en Conseil d'administration du 24 novembre 2023 ;*
VU *la délibération CA-2025-ÉLECTION-UPEC-65 en date du 3 octobre 2025 par laquelle le Conseil d'administration a élu Madame Karine Bergès à la présidence de l'Université Paris-Est Créteil Val-de-Marne (UPEC) ;*
VU *la présentation de la charte relative à l'usage de l'intelligence artificielle au sein de l'université présentée en conseil d'administration et annexée à la présente délibération ;*

Le Conseil d'administration de l'Université Paris-Est Créteil Val-de-Marne (UPEC), après en avoir délibéré :

ARTICLE 1 :

Approuve la charte de l'usage de l'intelligence artificielle au sein de l'université telle que définie dans les documents en annexe.

ARTICLE 2 :

La présente délibération sera transmise au Recteur Chancelier des Universités. Elle sera publiée conformément aux dispositions relatives à la publication des actes à caractère réglementaire de l'Université Paris-Est Créteil Val-de-Marne (UPEC).

La directrice générale des services est chargée d'exécuter la présente délibération.

Fait à Créteil, le 13 mars 2026

Le Vice-Président du Conseil d'Administration

Amilcar BERNARDINO

La Présidente de l'Université

Karine BERGÈS

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

UPEC
Connaissance - Action

UNIVERSITÉ PARIS-EST CRÉTEIL VAL DE MARNE

DÉLIBÉRATION

Le Conseil d'Administration de l'Université réuni en formation plénière le 13 mars 2026

Nombre de membres constituant le conseil : 32 **Nombre de membres en exercice : 32** **Quorum : 17** Membres présents : 17 Membres représentés : 7 **Total des membres présents et représentés : 24**	**DÉCOMPTE DES VOIX** Votants : 24 **Votes exprimés : 24** Pour : 14 Contre : 0 Abstentions : 10

Modalités de recours *: La présente délibération peut faire l'objet d'un recours pour excès de pouvoir dans un délai de deux mois à compter de sa publication et de sa transmission au Recteur d'académie.*

DAJG/FH DIRECTION DES AFFAIRES JURIDIQUES ET GENERALES, 61, avenue du Général de Gaulle - 94010 Créteil
Tél. +33 (0)1 45 17 10 31 conseilsetcommissions@u-pec.fr

Charte de l'Université Paris-Est Créteil sur le bon usage de l'Intelligence artificielle ("IA")

Préambule

La démocratisation de l'intelligence artificielle, et notamment celle de l'intelligence artificielle générative (IAg)[1] constitue une avancée technologique majeure dont se sont d'ores et déjà emparés les membres de la communauté universitaire, notamment dans le cadre de leur vie privée.

Désormais, l'utilisation de l'intelligence artificielle (IA) est susceptible de transformer en profondeur les pratiques pédagogiques, scientifiques, administratives et organisationnelles dans l'enseignement supérieur et plus spécifiquement dans l'université.

Ces outils IA offrent des opportunités significatives en matière d'apprentissage personnalisé, de soutien à la recherche, de production de contenus, ou encore de facilitation de certaines tâches, voire de leur automatisation.

Cependant, leur usage soulève également des enjeux importants, notamment :

- **juridiques** (respect du droit d'auteur, du Règlement général de la protection des données (RGPD), du Règlement européen de l'intelligence artificielle (RIA[2], AI Act), des évaluations de conformité référentiel général de sécurité (RGS), de la prévention de la fraude académique, etc.),
- **technologiques** (biais algorithmiques, sécurité des données, exactitude des résultats, etc.),
- **éthiques** (transparence, intégrité, responsabilité dans l'usage, bienveillance, etc.),
- **psychosociaux** (risques liés à l'isolement, à la surcharge cognitive, à la désinformation ou à la perte de sens du travail, à une nouvelle approche de certaines tâches, voire de certains métiers), et des enjeux psychosociaux pouvant comporter les risques liés à l'accoutumance ou à la dépendance aux outils d'IA,
- **organisationnels** (formations, sensibilisation, évolutions des postes et des missions de la communauté universitaire, etc.),
- **de développement durable et de responsabilité sociétale** (minimisation de l'utilisation de l'IA, utilisation autant que faire se peut de solutions plus frugales).

Afin d'accompagner ces transformations, tout en garantissant un usage conforme aux finalités éducatives, de recherche et aux valeurs du service public, l'Université Paris-Est Créteil a décidé de se doter de la présente charte, qui fixe les principes et règles qui encadrent l'utilisation de l'intelligence artificielle au sein de l'établissement.

Elle s'inscrit dans le cadre des articles L.123-2, L.123-3, L123-4-1 et L123-4-2 du Code de l'éducation, qui rappellent les missions humanistes, critiques et démocratiques de l'enseignement supérieur. Elle engage

[1] Afin de garantir la clarté et la cohérence des termes employés, nous avons choisi d'utiliser le terme « intelligence artificielle » (IA) dans son acception générique pour désigner l'ensemble des technologies et systèmes reposant sur des mécanismes d'intelligence artificielle, qu'ils soient symboliques, apprenants, génératifs, hybrides ou robotiques.
Lorsque la présente charte fait référence spécifiquement aux systèmes d'intelligence artificielle capables de générer du contenu de manière autonome (textes, images, sons, code, etc.), nous utilisons le terme « intelligence artificielle générative » (IAg).
Cette distinction terminologique vise à faciliter la compréhension des enjeux propres à chaque catégorie de technologies et à encadrer leur usage de manière adaptée.

2 Règlement européen de l'intelligence artificielle (AI Act) est un règlement adopté par l'Union européenne en 2024. Il constitue le premier cadre juridique complet au monde consacré à l'intelligence artificielle (IA). Il vise à encadrer la conception, le développement, la mise sur le marché et l'utilisation des systèmes d'IA dans l'UE, en garantissant la sécurité et le respect des droits fondamentaux.

l'ensemble des usagers – étudiants, enseignants, chercheurs, personnels administratifs et techniques, à adopter une posture responsable et critique vis-à-vis de ces technologies.

À caractère normatif, la présente charte est annexée au règlement intérieur de l'établissement. À ce titre, son respect est obligatoire et tout manquement aux dispositions identifiées comme obligatoires peut entraîner des mesures prévues par les dispositions disciplinaires en vigueur.

Les dispositions identifiées comme "obligatoires » ont un caractère normatif et s'imposent à l'ensemble des usagers.

Les dispositions présentées comme recommandations ou bonnes pratiques ont une valeur indicative et pédagogique ; leur non-respect ne peut, à lui seul, fonder une sanction disciplinaire.

Cette charte du bon usage de l'IA complète la charte du bon usage des moyens informatiques de l'Université Paris-Est Créteil.

Elle repose sur huit principes fondamentaux :

- La curiosité et la recherche de l'innovation et de la création, en s'appuyant sur l'intérêt et l'engagement des utilisateurs ;
- La transparence, en s'assurant que les processus mis en œuvre et les résultats obtenus sont compréhensibles ;
- La confidentialité, notamment des données à caractère personnel et des informations constituant le patrimoine informationnel de l'Université ;
- L'éthique, l'intégrité scientifique, la déontologie et le respect du principe de licéité ;
- La prudence, en encadrant certaines actions pour se prémunir de conséquences indésirables ;
- L'évitement, en refusant certains usages pouvant avoir des conséquences inacceptables, par exemple contraires aux lois et à la réglementation en vigueur, ainsi qu'aux principes éthiques en vigueur (dignité humaine, ordre public, respect des droits fondamentaux …) ;
- La parcimonie et la sobriété, notamment afin de minimiser l'impact environnemental de ces outils ;
- La traçabilité : en documentant et déclarant tout usage.

Elle vise ainsi à placer l'humain au cœur des préoccupations du développement de l'IA et de son utilisation.

Elle s'adresse à tous les utilisateurs de l'Université qu'ils soient étudiants ou personnels enseignants, enseignants-chercheurs, chercheurs ou personnels administratifs, techniques et assistants sociaux en charge d'une fonction support, soutien ou de direction. Elle ne saurait concerner les usages de l'IA dans le cadre d'activités privées, ces dernières devant être réalisées sur des systèmes d'infrastructures personnels, sans référence aux identifiants du compte numérique UPEC. Elle prend en compte les opportunités et les risques inhérents à tout outil d'IA. Elle s'applique à l'utilisation d'IAg, comme à tout système propre que l'Université mettrait en service.

Cette charte comporte des exigences exprimées sous la forme d'obligations et d'interdictions.

Elle invite à une attention particulière compte tenu de la jeunesse de nombreuses technologies et encourage toutes les parties prenantes à proposer des compléments et adaptations à la présente charte.

La charte est évolutive dans le cadre d'un processus d'amélioration continue. Chaque usager doit se tenir informé des évolutions de la charte et du droit applicable.

Article 1 : exigences pour l'utilisateur d'une IA

1.1. Usage raisonné et esprit critique

Chaque utilisateur est tenu d'utiliser l'IA avec discernement et parcimonie en appréciant les opportunités et les limites et menaces de l'usage qu'il en fait. Cette utilisation ne peut en aucun cas se substituer à un travail de réflexion personnelle et d'analyse. L'utilisateur doit donc maîtriser son sujet avant de formuler une requête à une IA. Chaque utilisateur est tenu de veiller à maintenir un usage mesuré et critique des outils d'IA afin d'éviter toute situation de dépendance ou d'accoutumance susceptible d'altérer son autonomie intellectuelle, son jugement personnel et ses capacités professionnelles.

1.2. Finalités et cadre d'usage

Il est tenu :

- D'utiliser l'IA comme outil d'appui et non de substitution à ses responsabilités ;
- De privilégier les outils validés par l'Université et conformes notamment au Règlement général sur la protection des données (RGPD), au règlement européen sur l'intelligence artificielle (AI Act ou RIA) et au Référentiel général de sécurité (RGS),
- De garantir la confidentialité, la sécurité et l'intégrité des données traitées.

1.3. Vérification et fiabilité des contenus

Chaque utilisateur doit avoir conscience qu'une IA repose notamment sur un fonctionnement statistique et probabiliste qui produit des contenus plausibles. Ceux-ci peuvent être exacts, mais aussi partiellement inexacts, voire entièrement faux (biais, hallucinations ...), de manière volontaire ou involontaire.

Ainsi des risques d'existence de biais de création, par exemple provenant de la reprise de certains préjugés, de stéréotypes, de partis pris, de conformisme, voire de propos diffamatoires ou racistes, sont possibles.

Chaque utilisateur est tenu de vérifier les propositions, les références et les faits énoncés par le système d'IA qu'il utilise.

Article 1.4 – Outils d'intelligence artificielle et respect des règles de sécurité

L'usage des systèmes d'intelligence artificiel est apprécié au cas par cas, en fonction :

- de la sensibilité des données traitées ;
- de la finalité de l'usage envisagé (enseignement, évaluation, recherche, gestion) ;
- et des effets potentiels sur les personnes et l'institution.

Il repose sur un principe de graduation des risques dit du *« feu tricolore »*, indépendamment de toute validation générale et définitive des outils, dont les conditions d'utilisation, politiques de confidentialité et modalités de traitement des données sont par nature évolutives.

En toute hypothèse, l'utilisateur demeure tenu de respecter les dispositions prévues à l'article 1.5 de la présente Charte.

🔴 usages interdits

Il est strictement interdit de saisir ou de traiter, au moyen d'outils d'IA accessibles au public ou non encadrés contractuellement, notamment les versions gratuites ou grand public :

- des données personnelles (noms, prénoms, adresses électroniques, identifiants, notes, appréciations) d'étudiants ou de personnels ;
- des données sensibles au sens du RGPD (santé, handicap, données sociales, RH…) ;
- des données confidentielles ou stratégiques de l'Université, notamment :

    - données financières ou budgétaires,
    - procédures disciplinaires ou contentieuses,
    - données de sécurité des systèmes d'information,
    - données de recherche non publiées ou couvertes par un contrat ou un accord de confidentialité.

Exemples universitaires (interdits) :

- transmettre des copies d'examen à une IA grand public ;
- analyser des notes ou des listes d'étudiants avec un outil externe ;
- soumettre des résultats de recherche non publiés à une IA en ligne.

🟡 usages tolérés

Il est toléré, sous la responsabilité exclusive de l'utilisateur, de recourir à des outils d'IA grand public pour des usages non critiques, à condition que seules soient traitées :

- des données publiques ;
- ou des données anonymisées (sans possibilité de ré-identification).

Ces usages ne doivent :

- produire aucun effet décisionnel (note, validation, orientation, sanction) ;
- ni se substituer à une appréciation humaine.

L'utilisateur demeure tenu :

- de vérifier les résultats produits ;
- d'en apprécier la pertinence, la fiabilité et la conformité aux règles pédagogiques, scientifiques et juridiques applicables.

Exemples universitaires (tolérés)

    - reformuler un support de cours déjà publié ;
    - générer des exercices ou QCM d'entraînement ;
    - résumer un texte réglementaire ou scientifique public.

🟢 usages recommandés

Il est recommandé, pour tout usage professionnel impliquant :

- des données sensibles ou structurantes ;
- des traitements à enjeux pédagogiques, scientifiques ou organisationnels ;
- ou des usages susceptibles d'avoir un impact sur les personnes,

De recourir exclusivement :

- aux outils d'IA mis à disposition par l'université ;

- ou à des outils ayant fait l'objet d'une mise en conformité préalable, notamment au regard :
    - du RGPD,
    - du règlement européen sur l'intelligence artificielle (AI Act),
    - des exigences de sécurité,
    - et de l'encadrement contractuel.

Usages à risque élevé

Les usages d'IA présentant un niveau de risque élevé, en particulier dans les domaines :

- de l'évaluation, de la notation, de la certification ou de l'orientation ;
- de la gestion des ressources humaines, financières, médicales ou sociales ;
- du suivi individualisé des étudiants ou des personnels…

sont impérativement soumis à une appréciation et un encadrement institutionnels spécifiques, incluant, selon les cas, la saisine du DPO, du RSSI ou du « comité de suivi éthique & numérique-IA » (COSUI) (cf. article 8 de la présente charte).

Le niveau de risque d'un usage d'intelligence artificielle dépend moins de l'outil utilisé que de la nature des données traitées et des effets produits.

En cas de doute, l'utilisateur doit s'abstenir et solliciter un avis institutionnel préalable.

1.5. Gestion et protection des données

Dans le même sens, chaque utilisateur est tenu de s'interroger sur les caractéristiques des données utilisées (personnelles, confidentielles, administratives, soumises à l'obligation de réserve ...), et est tenu de se contraindre à un usage minimisé de ces dernières. Les données traitées doivent être strictement proportionnées à la finalité recherchée.

Ainsi, lorsqu'un système conduit à transmettre des informations à l'extérieur de l'Université, chaque utilisateur est tenu d'apprécier les conséquences de la sortie de ces informations pour protéger le patrimoine informationnel de l'Université et respecter les lois et règlements.

En particulier, chaque utilisateur s'interdit de transmettre à une IA des informations protégées par des droits de propriété intellectuelle, ou sur lesquelles s'applique un devoir de réserve, une obligation de discrétion ou de neutralité, ou un respect du secret professionnel.

Un utilisateur qui soumettrait une nouvelle méthode ou une invention non encore protégée à une IA extérieure prendrait le risque de ne plus pouvoir la protéger par la suite. Chaque utilisateur est tenu d'avoir conscience que le meilleur moyen de protéger ses informations est de ne pas les transmettre à un système d'IA. Il doit être conscient qu'à ce jour, en France, une œuvre entièrement générée par une IA n'est pas protégée au titre du droit d'auteur.

1.6. Conformité légale et protection des données personnelles

Chaque utilisateur s'interdit d'utiliser des solutions d'IA sans avoir vérifié que le traitement et l'hébergement sont conformes aux lois et règlements européens sur la protection des données, notamment s'il existe des transferts d'informations à caractère personnel en dehors de l'Espace Economique Européen. (Cf. Annexe n°1)

Chaque utilisateur est tenu de vérifier que les contenus générés, y compris les images, les sons et les vidéos, ne contiennent pas de données à caractère personnel reconnaissables, ou permettant de contribuer de manière insidieuse à l'identification d'une personne.

1.7. Respect de la propriété intellectuelle et de l'intégrité scientifique

Chaque utilisateur s'interdit de s'attribuer un titre d'auteur pour un contenu généré par une IA, à partir de documents écrits par d'autres. Une telle pratique constituerait un manquement grave à l'intégrité professionnelle, pédagogique ou scientifique. La dissimulation de la véritable contribution serait porteuse de risques de plagiat. Chaque utilisateur d'une IA est tenu de préciser dans le contenu produit par l'IA les sources de ses informations.

1.8. Information et consentement des participants

Au commencement d'une réunion, notamment lors d'une visioconférence, chaque utilisateur souhaitant utiliser une IA doit en informer préalablement les participants et recueillir leur consentement pour effectuer un traitement des données tel que l'enregistrement de la réunion ou tout autre traitement transcription...). Cette règle s'applique aussi si une IA est l'un des invités à une visioconférence.

1.9. Validation et responsabilité des contenus générés

Chaque utilisateur est tenu de valider et vérifier les contenus générés par une IA en procédant lui-même à une relecture attentive et critique, ou le faisant faire par une autre personne humaine. Il doit assumer la pleine responsabilité des contenus générés, même si ceux-ci comportent des erreurs.

L'utilisateur, lors de la conception d'une application ou d'un système, est tenu de prendre en compte la protection de la vie privée, ainsi que les règles de sécurité en vigueur et prévoir un paramétrage par défaut qui en tienne également compte.

L'utilisateur qui recourt à une IA pour générer du code informatique demeure responsable de sa qualité et de sa sécurité. À ce titre, il doit vérifier que le code est documenté, testé et conforme aux standards de développement applicables, et s'assurer qu'il répond aux exigences fonctionnelles définies.

1.10. Respect du cadre légal, moral et éthique

La liberté d'expression et les libertés académiques s'appliquent y compris pour l'usage des contenus produits par une IA. Chaque utilisateur est tenu également de respecter les limites de ces libertés, telles que définies par la loi, le règlement, ou encore par la moralité, l'éthique et la déontologie.

Ainsi, l'utilisation d'une IA est interdite pour créer de faux contenus (texte, image, audio et vidéo) pouvant être juridiquement caractérisés d'injure, de diffamation, d'incitation à la violence ou à la haine, de discrimination ou de harcèlement de toute nature. Il en est de même de contenus créés à des fins frauduleuses, par exemple pour usurper une identité, ou créer de fausses identités, ou produire de faux documents.

1.11. Sobriété numérique et impact environnemental

Chaque utilisateur doit également avoir conscience que les IA sont très consommatrices de ressources matérielles et énergétiques. L'empreinte carbone que génère l'IA doit conduire chaque utilisateur à raisonner les usages qu'il veut en faire. Il doit être attentif aux possibilités d'utilisation d'autres solutions moins énergivores : effectuer une requête avec un moteur de recherche classique plutôt qu'une IA, voire une IAg, ou recourir à une banque d'images existantes plutôt que générer une nouvelle image, par exemple.

Article 2 : exigences pour la conception ou le déploiement d'une IA

2.1. Principes généraux de transparence, de confidentialité et d'éthique

Comme il est indiqué à travers la liste des principes énoncés en introduction, chaque concepteur[3] ou personne chargée de déployer une IA est tenu de respecter, tant pour l'enseignement que pour la recherche, les principes de transparence concernant son utilisation, la confidentialité, ainsi que l'éthique et l'intégrité scientifique.

2.2. Analyse d'impact préalable pour les systèmes à haut risque[4]

En tout état de cause, chaque personne chargée de déployer une IA traitant de domaines et/ou d'usages à haut risque au sens du Règlement européen de l'intelligence artificielle (RIA), est tenue, préalablement à sa mise en place, de procéder à une analyse d'impact (relative aux droits fondamentaux, incluant celle sur la protection des données). Ce travail doit être fait de manière concertée et collaborative.

2.3. Suivi continu et audits de conformité

Chaque concepteur ou personne chargée de déployer une IA est tenu d'assurer un suivi continu et des audits pour garantir la conformité aux exigences du règlement.

2.4. Maintien du rôle et de la supervision humaine

Chaque concepteur ou personne chargée de déployer une IA veille à concevoir et mettre en œuvre une technologie d'IA qui s'appuie sur l'intervention humaine et demeure sous son contrôle.
Il est tenu de s'assurer que le système proposé complète, prolonge ou amplifie l'action humaine, dans le respect du principe de supervision et de maîtrise humaines.

2.5. Compréhension et consentement des utilisateurs

Chaque concepteur ou personne chargée de déployer une IA est tenu de s'assurer de la compréhension de celle-ci par ses futurs utilisateurs, préalablement informés et recueillir leur consentement quand celui-ci est requis

[3] **Concepteur :** Toute personne physique ou morale qui conçoit un système d'IA et en assure le développement initial.
[4] Cf. annexe III du RIA et glossaire.

2.6. Base légale et encadrement du traitement des données personnelles

Le responsable du traitement[5] est tenu de procéder au traitement de données personnelles en s'appuyant sur une base légale appropriée, adaptée à la situation et au type de traitement concerné. Cette base légale devra être définie en amont du traitement des données personnelles avec la cellule DPO [6]de l'établissement.

2.7. Sécurité et cloisonnement des données d'entraînement

Chaque concepteur ou personne chargée de déployer une IA est tenu de s'assurer que les données d'entraînement[7] sont protégées avec un niveau approprié de sécurité. En particulier, un cloisonnement des données doit être mis en place avec des environnements dédiés, lorsque cela est nécessaire, au cours de chaque phase de déploiement d'une IA.

2.8. Interdiction du réentraînement des modèles

Chaque concepteur ou personne chargée de déployer une IA s'interdit de réentraîner[8] un modèle de manière non supervisée par un humain. Toutefois, l'université ou un organisme de recherche partenaire, agissant en qualité de concepteur, peut envisager un réentraînement dans le cadre d'un protocole scientifique ou pédagogique rigoureusement encadré, à condition que ce processus fasse l'objet d'une supervision humaine explicite, documentée et conforme aux principes éthiques et réglementaires en vigueur.

2.9. Interdictions prévues par le Règlement européen (RIA – article 5)

Chaque concepteur ou personne chargée de déployer une IAg est tenu d'avoir conscience que le Règlement européen sur l'intelligence artificielle (AI Act ou RIA), en son article 5 interdit formellement :
- Le recours à des techniques subliminales, délibérément manipulatrices au-dessous du seuil de conscience d'une personne ou des techniques délibérément manipulatrices ou trompeuses pour altérer substantiellement son comportement ou ses prises de décision d'une manière qui cause ou est susceptible de causer un préjudice important à cette personne ou à des tiers.

- Une IA exploitant des vulnérabilités liées à l'âge, au handicap ou à la situation économique ou sociale spécifique de certaines personnes, avec pour objectif ou effet d'altérer leurs comportements d'une manière qui cause ou est susceptible de causer un préjudice important à cette personne ou à un tiers.
- Les systèmes pour l'évaluation ou la classification de personnes en fonction de leur comportement social, de caractéristiques personnelles ou de personnalités connues conduisant à un traitement préjudiciable de

---

[5] **Responsable de traitement :** personne physique ou morale, autorité publique, organisme ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles. En d'autres termes, c'est la partie qui décide pourquoi et comment les données personnelles doivent être collectées et traitées. Cette personne ou entité porte la responsabilité juridique du respect des règles de protection des données dans le cadre du traitement. (Cf. article 4, §7 du RGPD).

[6]dpo@u-pec.fr

[7] **Entraînement d'une IA** : Processus de préparation d'un modèle comprenant :

- La collecte et préparation des données à partir de vastes ensembles,
- Le choix d'un algorithme et d'un modèle,
- L'exposition du modèle aux données d'entraînement pour ajuster ses paramètres,
- Le test du modèle sur un jeu de données distinct pour évaluer ses performances.

[8] **Le réentraînement** (ou **retraining**) : Processus par lequel un modèle d'intelligence artificielle ou d'apprentissage automatique est réentraîné sur un nouvel ensemble de données, ou sur des données mises à jour, afin d'améliorer sa performance, de corriger des erreurs, de s'adapter à de nouvelles conditions, ou de prendre en compte des évolutions dans les données ou le contexte

personne dans un contexte dissocié de celui dans lequel les données ont été collectées ou générées, ou qui est injustifié ou disproportionné.
- Les systèmes IA pour mener des évaluations ou des prédictions de risques qu'une personne future commette une infraction pénale sur la seule base d'un profilage ou de l'évaluation de traits de personnalité et de ses caractéristiques.

- Les systèmes d'IA qui créent ou développent des bases de données de reconnaissance faciale par l'extraction non ciblée d'images faciales.
- Les systèmes d'IA qui déduisent les émotions d'une personne sur son lieu de travail ou dans les établissements d'enseignement (sauf pour une utilisation pour raisons médicales ou de sécurité).

- Les systèmes d'IA qui classent individuellement les personnes sur la base de leurs données biométriques afin de déduire ou d'inférer leur origine ethnique, leurs opinions politiques, leur appartenance syndicale, leurs croyances religieuses ou philosophiques, leur vie ou orientation sexuelle.

- Les systèmes d'IA d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins de maintien de l'ordre.

2.10. Qualification des systèmes à haut risque dans l'éducation et la formation

Chaque concepteur ou déployeur d'un système d'intelligence artificielle est tenu d'avoir conscience que, conformément aux articles 6 et suivants et à l'annexe III du règlement (UE) 2024/1689 sur l'intelligence artificielle (AI Act- RIA , les systèmes d'intelligence artificielle utilisés dans le domaine de l'éducation et de la formation sont susceptibles d'être qualifiés de systèmes à haut risque lorsqu'ils produisent ou influencent de manière déterminante des décisions relatives à l'accès à une formation, à l'évaluation des performances ou à l'orientation des apprenants.

L'Université distingue, à ce titre, deux catégories d'usages pédagogiques :

1/ Usages d'assistance (en principe à risque limité)

Les usages d'assistance, tels que l'aide à la conception de cours, la génération d'exercices ou de supports d'entraînement, sont autorisés dès lors qu'ils n'emportent aucun effet décisionnel sur le parcours de l'étudiant et qu'ils font l'objet d'une vérification humaine.

2/ Usages décisionnels (à haut risque)

Les usages décisionnels, notamment ceux déterminant l'accès à une formation, l'attribution d'une note, la validation de compétences ou l'orientation des apprenants, relèvent d'un régime renforcé. Ils sont subordonnés à une supervision humaine effective, à l'absence de décision exclusivement automatisée au sens de l'article 22 du RGPD, à la réalisation des analyses d'impact requises et à un encadrement institutionnel préalable.

La saisine du délégué à la protection des données (DPO) est obligatoire dès lors qu'un usage implique des données personnelles ou une évaluation certificative, celle du responsable de la sécurité des systèmes d'information (RSSI) dès lors qu'un outil externe ou un traitement sensible est envisagé et questionne sur les aspects « sécurité du système d'information ou la souveraineté », et celle du « comité de suivi éthique & numérique-IA » (COSUI), lorsque l'usage relève d'un système à haut risque ou présente des enjeux éthiques, pédagogiques ou institutionnels. En qualité de déployeur, l'Université veille au respect des obligations de supervision humaine, de gestion des risques, de traçabilité et de conformité prévues par le règlement sur l'intelligence artificielle.

2.11. Mesures à prendre et obligations associées

À ce titre, pour déterminer les mesures à prendre, le concepteur ou le déployeur doit :

- Vérifier la qualification du système,
- Se rapprocher du DPO pour la conformité au RGPD,
- Consulter le RSSI pour les mesures de sécurité,
- Respecter les obligations légales applicables aux systèmes à haut risque (documentation, gestion des risques, supervision humaine, sécurité, transparence).

Le non-respect de ces obligations expose à d'importantes sanctions.

2.12. Validation institutionnelle et dépenses

Tout engagement de dépenses institutionnelles relatif à des outils d'intelligence artificielle à usage professionnel est subordonné à une appréciation préalable des usages envisagés, des obligations de conformité applicables et des impacts budgétaires, et fait l'objet d'une validation par la Présidence après instruction par le Comité de Régulation du Numérique (CORéNUM).

Article 3 : exigences pour la pédagogie et la formation

Chaque enseignant peut recourir à des systèmes d'intelligence artificielle dans le cadre de ses activités pédagogiques, à titre d'outil d'appui et de complément à son expertise. Il veille en toutes circonstances à conserver la maîtrise des contenus, des évaluations et des interactions pédagogiques, ainsi qu'à garantir la qualité, la fiabilité et la pertinence des apports issus de l'IA.

L'usage de l'intelligence artificielle doit demeurer encadré par la supervision, le discernement et la responsabilité professionnelle de l'enseignant. Celui-ci est tenu de veiller à pouvoir assurer la continuité de son enseignement indépendamment de tout recours à l'IA.

L'enseignant est tenu d'informer de manière explicite et formelle les étudiants des règles applicables à l'usage de l'IA, y compris des éventuelles restrictions dans le cadre des activités pédagogiques.

Enfin, l'enseignant est encouragé à favoriser auprès des étudiants une utilisation critique, raisonnée et éthique des outils d'intelligence artificielle, en les sensibilisant aux enjeux de fiabilité, d'autonomie et de développement de leur esprit critique.

Article 4 : exigences pour les évaluations des travaux des étudiants

Dans le cadre du Règlement européen sur l'intelligence artificielle (AI Act ou RIA), l'usage de l'IA à des fins d'évaluation des étudiants est considéré comme un usage à haut risque. Ce classement implique des obligations strictes pour l'établissement et pour l'enseignant en sa qualité de responsable pédagogique.

L'établissement, avant la mise en service du système d'IA à haut risque et avant de permettre à l'enseignant de l'utiliser, est tenu de respecter les exigences suivantes :

- Une analyse d'impact des droits fondamentaux, à savoir l'utilisation de l'IA est-elle susceptible de porter atteinte à la vie privée, à l'équité, à la non-discrimination, etc. ;
- Dans le cadre de l'obligation de transparence et d'information, les étudiants doivent être clairement informés que l'IA est utilisée dans l'évaluation. Ils doivent savoir quand, comment, et dans quelle mesure elle intervient ;
- Dans le cadre de l'obligation de traçabilité et de documentation, l'IA utilisée doit permettre un audit a posteriori : chaque action ou décision prise par l'IA doit pouvoir être retracée ;
- Une supervision humaine est obligatoire. Ainsi l'enseignant doit pouvoir comprendre et corriger les décisions ou suggestions de l'IA. Il reste ultimement responsable.

Chaque enseignant désireux d'utiliser l'IA en vue de l'évaluation des connaissances et des compétences acquises par ses étudiants est tenu d'utiliser un système IA autorisé par l'établissement pour l'usage identifié dans le respect de la conformité aux exigences du RIA et le cas échéant conformément aux règles relatives à l'encadrement des examens.

Chaque enseignant est responsable du cadre de l'évaluation des apprentissages et c'est dans ce cadre qu'il autorise, ou non, l'utilisation des IA.

Les étudiants sont tenus de respecter ce cadre d'évaluation défini par l'enseignant.

Chaque étudiant, dans le cadre des évaluations de connaissances et de compétences, ne peut produire un travail, en tout ou partie, à l'aide d'un système d'intelligence artificielle qu'avec l'autorisation expresse et préalable de l'enseignant, dans le cadre défini par celui-ci. Tout usage non autorisé constitue une fraude caractérisée et expose l'étudiant aux sanctions disciplinaires prévues par la réglementation en vigueur.

Dans les cas où l'usage est autorisé, chaque étudiant doit déclarer lors d'une évaluation les passages concernés par l'utilisation d'une IAg.

En cas de non-déclaration ou d'usage non autorisé de l'intelligence artificielle, la fraude peut être caractérisée soit par la violation des règles applicables à l'évaluation, soit par l'incapacité de l'étudiant à expliquer, justifier ou maîtriser son raisonnement, sa méthodologie ou le contenu de sa production, notamment lors d'une interrogation orale ou écrite.

Les outils de détection de contenus générés par IA ne peuvent constituer qu'un indice ou un élément d'alerte, et ne sauraient, à eux seuls, constituer une preuve suffisante de fraude.

Toute procédure disciplinaire engagée à ce titre est conduite dans le respect des dispositions légales et réglementaires en vigueur, du principe du contradictoire et des droits de la défense.

Article 5 – Exigences générales et spécifiques en matière d'usage de l'IA dans la recherche

5.1 Principes généraux

Chaque utilisateur d'une IA dans le cadre de travaux de recherche est tenu de s'assurer qu'il préserve la confidentialité et la valeur stratégique de l'information lorsqu'il utilise une IA.

À ce titre, tout chercheur est tenu de s'abstenir d'introduire dans un système d'IA externe non validé des données sensibles ou protégées (résultats non publiés, codes sources, données personnelles, stratégiques ou appartenant à l'Université et/ou à ses partenaires). Il est tenu de protéger le patrimoine scientifique, technique et informationnel de son établissement et de respecter les obligations contractuelles attachées aux projets de recherche (accords de consortium, conventions de tutelle, financements…).

Chaque utilisateur d'une IA doit toujours vérifier les sources d'un contenu généré par une IA et ajouter les références appropriées lorsque nécessaire. Lorsqu'il existe une innovation, il doit mentionner l'IA utilisée sur tout ou partie du contenu généré.

Chaque utilisateur d'une IA s'interdit de dissimuler l'utilisation d'une IA dans la création d'un contenu ou la rédaction d'une publication, lorsque celle-ci a contribué de manière substantielle à la création d'un contenu. Il doit être conscient qu'un tel fait est un manquement à l'intégrité scientifique.

Chaque utilisateur d'une IA s'interdit de fabriquer avec une IA des données de recherche qui permettraient de falsifier des résultats[9].

Chaque utilisateur d'une IA doit s'interdire d'utiliser une IA comme substitut à son activité de recherche, sans supervision ni vérification pour la production de contenus.

Dans le respect du principe de liberté académique et de la liberté de la recherche, chaque utilisateur demeure responsable des productions intellectuelles issues de ses activités. Le recours à des systèmes d'intelligence artificielle ne doit ni porter atteinte à cette liberté, ni altérer l'autonomie méthodologique du chercheur, ni créer une situation de dépendance à leur égard.

5.2 Application spécifique aux travaux académiques et scientifiques recourant à une IA générative

Chaque utilisateur recourant à une intelligence artificielle générative (IAg) dans le cadre d'un travail académique ou scientifique (mémoire, thèse, article, rapport de recherche, publication, etc.) demeure pleinement responsable du contenu produit par l'IA générative.

Chaque utilisateur est tenu de mentionner explicitement, dans le manuscrit ou la publication concernés, l'usage de l'IA générative, en indiquant l'outil utilisé, la finalité poursuivie (ex. : reformulation linguistique, traduction, aide à la structuration) et, le cas échéant, les passages concernés. La traçabilité de l'IA dans la recherche est assurée par une mention méthodologique explicite, conformément aux pratiques en vigueur dans les publications scientifiques.

Chaque utilisateur doit être en mesure de décrire la stratégie générale de « requêtes adressées au système d'IA » dite « prompting[10]» utilisée et/ou la méthodologie mise en œuvre le cas échéant, l'outil mobilisé ainsi que l'étendue de l'intervention de l'IA, en particulier lorsque cette stratégie joue un rôle significatif dans la démarche scientifique ou dans l'obtention des résultats. Lorsque cela est nécessaire et proportionné au regard de la nature du travail et des exigences de transparence ou de vérification scientifique, chaque utilisateur doit pouvoir justifier a posteriori les modalités de recours à l'IA.

Toute dissimulation de l'usage d'une IAg constitue un manquement à l'intégrité scientifique.

Chaque utilisateur peut avoir recours à une IAg pour des tâches de soutien limitées (correction stylistique, orthographique ou grammaticale, traduction, assistance à la structuration de plans ou de bibliographies).

Chaque utilisateur s'interdit d'utiliser une IAg pour :

- Rédiger intégralement ou substantiellement un chapitre ou une section scientifique ;
- Produire des données fictives ou falsifiées ;
- Substituer l'outil à la réflexion critique, à l'analyse méthodologique ou à l'argumentation scientifique personnelle.

[9] Code de la recherche : article L.211-2 (garantir la qualité et l'intégrité des travaux).
10 Le prompting est la pratique consistant à élaborer des requêtes structurées destinées à un système d'IA afin d'en déterminer ou d'en influencer le résultat.

Il est recommandé que chaque utilisateur conserve un journal d'IA retraçant les requêtes (« prompts »), les sorties générées et les corrections apportées, si ces derniers sont significatifs par rapport au contenu produit. Ce journal pourra être mis à disposition en cas de vérification[11].

Chaque utilisateur est tenu de vérifier l'exactitude des références, des citations et des données produites par l'IA et de les confronter systématiquement aux sources primaires (Légifrance, EUR-Lex, publications scientifiques, etc.).

Chaque utilisateur s'interdit de présenter comme original un contenu généré par IA qui reproduirait des œuvres protégées par le droit d'auteur[12]..

Tout manquement à ces règles peut être qualifié de fraude académique et entraîner les sanctions disciplinaires correspondantes, sans préjudice des actions civiles et pénales prévues en cas de contrefaçon.[13]

Chaque utilisateur est tenu de respecter les obligations de transparence prévues par le Règlement (UE) 2024/1689 dit « AI Act », qui qualifie les usages académiques et éducatifs de l'IA générative comme des usages à haut risque.

Article 6 : Exigences pour la gestion administrative (générale, RH, financière, sociale et/ou médicale)

6.1 Principes généraux

Chaque utilisateur relevant des fonctions de bibliothécaire, d'ingénieur, d'administratif, de technicien, de personnel social ou de santé (BIATSS), en sa qualité d'agent public, est soumis aux obligations générales du code général de la fonction publique : probité, neutralité, dignité, discrétion et confidentialité, loyauté et continuité du service public.

Dans l'exercice de ses missions de soutien à la formation, à la recherche, à l'administration et à la vie universitaire, chaque utilisateur peut avoir recours à des outils d'intelligence artificielle (IA). Cet usage doit demeurer strictement encadré afin de préserver la qualité du service public, la sécurité des données, le respect de la vie privée et la responsabilité humaine.

Chaque utilisateur est tenu :

- D'utiliser l'IA comme outil d'appui et non de substitution à ses responsabilités ;
- D'utiliser les outils validés par l'Université et des usages conformes au Règlement général sur la protection des données (RGPD), au Référentiel général de sécurité (RGS) et au Règlement européen sur l'intelligence artificielle (AI Act ou RIA) ;
- De garantir la confidentialité, la sécurité et l'intégrité des données traitées ;
- De préserver la qualité, l'accessibilité et l'équité du service rendu aux étudiants, aux enseignants-chercheurs et aux usagers.

Conformément à l'article 1, chaque utilisateur est tenu d'éviter toute dépendance aux outils d'IA afin de maintenir la maîtrise de ses missions et de préserver la dimension humaine des fonctions exercées.

[11] Ces éléments ne sont communicables qu'en cas de nécessité liée à une exigence de vérification scientifique ou de conformité réglementaire, et dans le respect des règles relatives à la protection des données et à la liberté académique.
[12] Code de la propriété intellectuelle notamment ses articles L.111-1 et L.113-1 (droits d'auteur).
[13] Code pénal notamment son article L.335-2 (sanctions pénales pour contrefaçon).

6.2 Application spécifique aux missions ci-dessous citées

A/ Personnels en charge des ressources humaines (RH)

Les personnels chargés des ressources humaines manipulent des données hautement sensibles concernant les agents de l'Université (dossiers de carrière, rémunération, situations individuelles, santé, discipline, etc.).

À ce titre, ils sont tenus :

- De garantir la confidentialité absolue de ces données ;
- De s'abstenir d'introduire des données nominatives ou personnelles dans des systèmes d'IA externes non validés ;
- De ne pas utiliser l'IA pour évaluer, sélectionner ou prédire le comportement ou les performances des agents ;
- De limiter l'usage de l'IA à des fonctions d'appui administratif (mise en forme de documents anonymisés, veille juridique et réglementaire) ;
- D'utiliser uniquement des outils d'IA respectant des conditions strictes de sécurité et de conformité.

B/ Personnels en charge de la gestion financière

Les personnels chargés de la gestion budgétaire et financière traitent des informations relatives aux marchés publics, contrats, budgets et factures, dont la confidentialité et la traçabilité sont essentielles.

Ils sont tenus de :

- De garantir la confidentialité et la traçabilité des données financières ;
- De s'abstenir d'introduire des informations budgétaires, contractuelles ou comptables dans des systèmes d'IA externes non validés ;
- De limiter l'usage de l'IA à des tâches d'appui telle que la veille réglementaire ;
- De faire vérifier et valider toute production issue de l'IA par un agent responsable ;
- De respecter strictement les règles de conservation, d'archivage et de traçabilité.

C/ Personnels en charge de missions sociales ou de santé

Les personnels exerçant des missions sociales, de santé ou en charge de la gestion des ressources humaines manipulent des données personnelles sensibles soumises à des obligations strictes de confidentialité.

- Les professionnels de santé sont soumis au secret médical, qui protège rigoureusement les données de santé des patients.
- Les travailleurs sociaux sont soumis au secret professionnel, garantissant la confidentialité des informations sociales.
- Les agents RH traitent des données personnelles sensibles relatives aux situations individuelles et à la santé des agents.

Ils sont tenus :

- D'assurer la confidentialité absolue des données traitées ;
- De garantir un cloisonnement et une sécurisation rigoureuse des traitements ;
- De limiter le recours à l'IA à des usages d'appui strictement encadrés ;
- De proscrire toute utilisation de l'IA visant à remplacer l'expertise humaine dans les processus décisionnels ou d'évaluation ;
- D'utiliser uniquement des outils d'IA respectant des conditions strictes de sécurité et de conformité aux normes applicables (RGPD, normes relatives aux dispositifs médicaux pour le secteur de la santé).

Article 7 : Responsabilités et sanctions

Chaque utilisateur et chaque concepteur d'un système d'intelligence artificielle est tenu de respecter les dispositions de la présente charte et d'agir en conformité avec celles-ci.

L'Université se réserve la faculté de conduire des audits de conformité à la charte, notamment par l'intermédiaire du délégué à la protection des données (DPO), du responsable de la sécurité des systèmes d'information (RSSI) ou de toute personne dûment mandatée à cet effet.

En cas de manquement avéré aux dispositions identifiées comme obligatoires de la présente charte, des procédures internes à l'Université peuvent être engagées, sans préjudice d'éventuelles responsabilités civiles ou pénales.

Il convient toutefois de rappeler que l'usage de l'IA constitue un champ encore émergent. Dans un premier temps, l'accent est mis sur la sensibilisation, la pédagogie et le dialogue avec l'ensemble des parties prenantes, afin de favoriser une appropriation progressive et partagée.

Les mécanismes d'audit et de sanction, bien que prévus, ne sont pas mis en œuvre de manière systématique dans cette phase initiale.

Article 8. Gouvernance et Révision

La charte est révisée régulièrement selon l'évolution du droit, des technologies, des recommandations scientifiques et éthiques et des usages. La révision de la charte est décidée dans le respect des procédures institutionnelles (à savoir après consultation et décisions des instances compétentes) selon des arbitrages éthiques et/ou politiques.

Toute révision :

- Est élaborée sur la base des retours d'expérience et de la veille ;
- Fait l'objet d'une version consolidée ;
- Est publiée et portée à la connaissance de la communauté universitaire ;
- Respecte le même processus de validation que la version initiale.

Une instance de gouvernance dédiée, le « comité de suivi éthique & numérique-IA » (COSUI), veille à la mise en œuvre et au respect de la charte. Elle exerce un rôle de conseil, de suivi et d'évaluation, notamment pour les projets intégrant des technologies d'intelligence artificielle, dans le respect des compétences des instances institutionnelles. Le comité peut, le cas échéant, proposer ou suggérer la saisine des instances compétentes lorsque la nature d'un projet ou d'une situation l'exige. (Cf. annexe 2)

Des audits peuvent être menés par l'auditeur interne, la cellule DPO, le RSSI ou toute autorité compétente.

Article 9. Accompagnement

La charte pourra être accompagnée :

- De chartes spécifiques initiées par les composantes de l'établissement et visant à décliner ses principes et cas d'usage en fonction de leur contexte ou besoins particuliers, dans le strict respect des dispositions de la présente Charte et de son corpus normatif ;
- De guides pratiques d'usage par profil métier ou autres items ;
- D'un plan de formation progressif ;

D'un espace de veille et de partage d'expériences

Article 10 : Dispositions finales

10.1 Portée et périmètre d'application

La présente Charte s'applique à l'ensemble de la communauté universitaire, dans le cadre des activités pédagogiques, scientifiques, administratives ou techniques conduites au sein de l'établissement.

Elle complète les textes et règles existants sans se substituer aux dispositions légales, réglementaires ou statutaires applicables, ni aux règles internes en vigueur.

10.2 Articulation avec le cadre institutionnel existant

La présente Charte s'inscrit dans le cadre du corpus normatif, réglementaire et déontologique de l'Université. À ce titre, elle s'articule notamment avec :

- Les statuts de l'Université ;
- Le Règlement intérieur, auquel la présente Charte est annexée et qui en assure l'opposabilité ;
- La Charte du bon usage des moyens informatiques ;
- La Politique de sécurité des systèmes d'information (PSSI) qui relève de l'autorité de la /du Président(e) de l'Université, autorité d'homologation. Sa mise en œuvre opérationnelle est assurée par le responsable sécurité du système d'information (RSSI), agissant par délégation.
- La Politique d'intégrité scientifique de l'Université qui est mise en œuvre sous l'autorité institutionnelle de l'Université, avec l'appui du comité d'éthique, de déontologie et d'intégrité scientifique (CEDIS), de la commission de la recherche et de la vice-présidence en charge de la recherche.

La présente charte ne se substitue pas à ces dispositifs, mais en précise l'articulation dans le contexte spécifique des usages de l'intelligence artificielle.

10.3 Cohérence et résolution des incohérences

La présente Charte est interprétée et appliquée en cohérence avec les dispositions légales et réglementaires ainsi qu'avec les textes internes avec lesquelles elle s'articule.

En cas d'incohérence ou de difficulté d'interprétation, il est fait application des dispositions de niveau supérieur et des règles les plus protectrices au regard des droits fondamentaux, de la protection des données et de la sécurité des systèmes d'information.

10.4 Validation et entrée en vigueur

La charte est adoptée sous réserve de la validation des instances compétentes (commission des statuts, comité social d'administration (CSA), commission de la recherche (CR), commission de la formation et de la vie universitaire (CFVU) et/ou conseil académique (CAC), conseil d'administration (CA).

Elle est annexée au règlement intérieur de l'établissement.

Elle entre en vigueur à compter de sa publication dans les espaces institutionnels de l'Université et est portée à la connaissance de l'ensemble des usagers par les moyens de communication internes habituels.

10.5 Statut des dispositifs d'accompagnement

Les dispositifs d'accompagnement mentionnés à l'article 9 ont un rôle d'appui et de facilitation. Ils ne créent pas de règles nouvelles et ne se substituent pas aux dispositions de la présente Charte ni aux prérogatives des instances universitaires.

ANNEXE 1-CRITERES DE CHOIX ET D'USAGE DES OUTILS D'INTELLIGENCE ARTIFICIELLE[1]

L'Université ne définit pas, à ce stade, de liste figée d'outils d'intelligence artificielle « autorisés », « tolérés » ou « interdits ».
L'usage des outils d'IA est apprécié au regard de la nature des données traitées, du contexte d'usage et des garanties offertes par l'outil, conformément au présent cadre.

Typologie recommandée

🟢 Outils d'IA utilisables

- IA sans saisie de données personnelles ou confidentielles,
- IA utilisées avec des contenus publics, génériques ou fictifs,
- IA configurées pour ne pas réutiliser les données (pas d'entraînement),
- IA conformes aux exigences RGPD (préférence UE/EEE).

❖ Usage pédagogique, rédactionnel, aide à la compréhension, reformulation générique.

🟡 Outils d'IA utilisables sous conditions

- IA nécessitant une analyse préalable des paramètres,
- IA utilisées dans un cadre pédagogique, scientifique ou administratif structuré,
- IA intégrées à un projet ou à un dispositif institutionnel.

❖ Saisine du Comité IA et/ou du DPO recommandée.

🔴 Outils d'IA interdits

- IA impliquant la saisie de données personnelles, sensibles ou confidentielles,
- IA réutilisant les données pour leur entraînement sans garantie,
- IA non conformes au RGPD ou hébergées hors UE sans encadrement,

---

[1]Le présent document a bénéficié d'une assistance rédactionnelle par un outil d'intelligence artificielle. Les analyses, arbitrages et validations relèvent exclusivement des responsables institutionnels.

- IA utilisées pour l'évaluation automatisée des étudiants ou des personnels.

❖ Interdiction stricte d'usage externe.

TABLEAU 1 – CONSEILS PRATIQUES POUR L'USAGE DES OUTILS IA

Règle	À faire (✅)	À éviter / interdit (❌)	Pourquoi ?
1. Données	Utiliser uniquement des données publiques ou génériques	Ne jamais saisir de données personnelles, sensibles, couvertes par le secret médical ou des affaires	Respect du RGPD et protection de l'UPEC
2. Identifiants	Utiliser les identifiants UPEC (SSO) seulement sur outils autorisés	Ne pas utiliser les identifiants UPEC sur outils interdits ou dans un cadre privé	Prévenir les risques de fuite et d'usurpation
3. Vérification	Relire et vérifier systématiquement les résultats	Copier-coller sans contrôle	L'IA peut se tromper (hallucinations, biais)
4. Transparence	Mentionner l'usage d'IA dans travaux et documents officiels	Passer sous silence l'usage de l'IA	Obligation de transparence (IA Act, règles académiques)
5. Contexte professionnel	Utiliser l'IA dans le cadre du temps de travail ou pédagogique	Usage excessif, détourné ou sans lien avec la mission	Bon usage des ressources de l'Université
Veille juridique	Consulter régulièrement une veille juridique (RGPD, IA Act, CNIL, doctrine, jurisprudence). L'Université met également en place une telle veille pour ses personnels et étudiants.	Ignorer les évolutions réglementaires et les mises à jour.	Anticiper les évolutions légales et rester en conformité.
7. Signalement	Alerter le DPO/RSSI en cas d'incident (données saisies par erreur)	Garder le problème pour soi	Traçabilité et correction rapide des incidents

TABLEAU 2 – PARAMETRES A ERIFIER ET/OU MODIFIER AVANT USAGE D'UNE IA

Paramètre	Réglage recommandé (✅)	À éviter / désactiver (❌)	Pourquoi ?
Entraînement des données	Activer le mode « Temporary Chat » ou refuser l'usage des prompts pour l'entraînement	Laisser l'option par défaut d'entraînement sur vos données	Protéger les données institutionnelles
Conservation	Activer la suppression automatique ou suppression manuelle régulière	Conserver un historique illimité	Minimiser les risques liés à la rétention
Sécurité du compte	Utiliser SSO UPEC sur outils autorisés, activer 2FA si disponible	Créer un compte perso pour usage pro	Conformité RGPD et sécurité institutionnelle
Partage	Désactiver les options de partage/publication par défaut	Rendre publics prompts et résultats	Prévenir les fuites d'informations
Localisation des données	Préférer un hébergement UE/EEE	Autoriser des transferts hors UE non encadrés	Respect du RGPD et limitation des risques
Traçabilité	Activer journaux d'usage (si proposés)	Pas de suivi des interactions	Conformité IA Act (traçabilité des systèmes)
Accessibilité	Vérifier conformité WCAG 2.2, activer options d'accessibilité	Ignorer ces paramètres	Inclusion et conformité réglementaire
Notifications de sécurité	Activer alertes de connexion et incidents	Désactiver les notifications	Prévenir les intrusions et incidents

UPEC
UNIVERSITÉ
PARIS-EST CRÉTEIL
VAL DE MARNE
Connaissance - Action

ANNEXE N°2 : « COMITE DE SUIVI ETHIQUE ET NUMERIQUE DES PROJETS PROPRE A L'INTELLIGENCE ARTIFICIELLE » (COSUI-IA).

1. Institution et missions

Il est institué une instance de gouvernance dédiée, dénommée « **Comité de Suivi éthique et numériques des Projets propre à l'Intelligence Artificielle » (COSUI-IA)**.

Cette instance a pour mission de veiller à la **mise en œuvre**, au **respect** et à la **bonne application** de la présente Charte du bon usage de l'IA de l'UPEC, ainsi qu'à l'**évaluation** des projets intégrant des technologies d'intelligence artificielle, notamment générative.

Elle exerce une fonction de **conseil, de suivi et d'évaluation**, et contribue à la **transparence**, à la **concertation** et à la **cohérence institutionnelle** des démarches entreprises dans le domaine de l'IA, en s'appuyant sur une approche **pluridisciplinaire et éthique**.

2. Rôle et attributions

Le COSUI-IA a pour principales attributions de :

- Assurer le **suivi régulier** de la mise en œuvre des projets liés à l'intelligence artificielle générative (IAG) dans l'établissement ;
- **Informer et associer** les différentes instances représentatives concernées (CSA, commissions pédagogiques, recherche, développement durable, etc.) selon les impacts constatés ou anticipés ;
- **Évaluer les effets** des projets IA sur les organisations, les missions, les compétences et les métiers ;
- **Examiner les impacts environnementaux et énergétiques** des projets IA, dans une logique de durabilité ;
- **Favoriser une approche transversale et décloisonnée** des enjeux IA, intégrant les dimensions techniques, humaines, éthiques, pédagogiques et écologiques ;
- **Proposer ou recommander**, le cas échéant, la **saisine des instances compétentes** lorsque la nature d'un projet ou d'une situation l'exige.

3. Composition

Le comité est composé de manière à refléter la pluralité des acteurs concernés par les usages de l'intelligence artificielle. Il comprend notamment :

- Des **représentants des directions concernées** (numérique, ressources humaines, développement durable, formation, communication) ;
- Des **représentants des personnels** ;
- Des **enseignants-chercheurs et formateurs**, impliqués dans les projets ou la réflexion autour de l'IA ;
- Des **représentants des usagers** (étudiants ou publics bénéficiaires) ;
- Le cas échéant, des **experts en intelligence artificielle, en éthique, en protection des données ou en sécurité numérique**, invités à titre consultatif.

4. Fonctionnement

Le comité :

- Se réunit à échéances régulières ou à la demande de la direction ou d'un membre en cas d'urgence ou de besoin d'alerte ;
- Informe régulièrement les instances centrales et peut **solliciter ou transmettre des avis** au CSA, aux conseils pédagogiques ou à d'autres organes consultatifs ;
- Produit des **restitutions documentées** : comptes rendus, fiches d'impact, recommandations, alertes ou retours d'expérience.

GLOSSAIRE ET DÉFINITIONS [1]

AIPD (Analyse d'impact relative à la protection des données) : Étude préalable visant à évaluer les risques qu'un traitement de données personnelles peut faire peser sur les droits et libertés des personnes concernées. Elle est requise lorsqu'un traitement est susceptible d'engendrer un risque élevé, notamment en cas d'usage de technologies nouvelles, de profilage ou d'évaluation systématique et approfondie. (Base légale : article 35 du RGPD).

Analyse de risque :Démarche méthodique consistant à identifier, qualifier et hiérarchiser les risques juridiques, scientifiques, contractuels, éthiques et institutionnels liés à l'utilisation d'un système d'intelligence artificielle. Dans le cadre du présent document, elle repose sur l'examen combiné de la nature des données, du contexte scientifique, des obligations contractuelles, du mode d'usage (outil institutionnel maîtrisé ou IA externe) et de l'impact potentiel en cas de divulgation, de transfert non maîtrisé ou de perte de souveraineté des données.

ANR (Agence Nationale de la Recherche) : Établissement public finançant des projets de recherche et pouvant imposer des obligations spécifiques en matière de diffusion, de valorisation, de confidentialité ou de localisation des données. Ces obligations s'imposent aux bénéficiaires et doivent être prises en compte avant toute transmission à une IA externe.

Anonymisation : Procédé technique rendant une donnée irréversiblement non identifiable par des moyens raisonnablement susceptibles d'être utilisés. Une donnée anonymisée sort du champ d'application du RGPD, sous réserve que l'irréversibilité soit effective. (Référence : considérant 26 du RGPD).

Assistance à la correction / Pré-correction : Usage d'un outil, éventuellement fondé sur l'intelligence artificielle, pour proposer des annotations, corrections ou pistes d'évaluation sans attribuer la note finale. La décision académique demeure humaine et ne peut être exclusivement automatisée. (Référence : article 22 RGPD).

Automatisation déterministe :Traitement algorithmique appliquant mécaniquement un barème ou une règle prédéfinie, sans apprentissage automatique ni inférence probabiliste. Un tel traitement ne constitue pas nécessairement un système d'intelligence artificielle au sens de l'article 3 du règlement européen sur l'IA.

Biais algorithmique : Résultat systématiquement déséquilibré, discriminatoire ou erroné produit par un système automatisé en raison des données utilisées, des paramètres retenus ou de la conception du modèle.

[1] [1] Le présent glossaire constitue un outil d'interprétation interne. Il ne se substitue pas aux textes législatifs et réglementaires en vigueur. Le présent document a bénéficié d'une assistance rédactionnelle par un outil d'intelligence artificielle. Les analyses, arbitrages et validations relèvent exclusivement des responsables institutionnels.

Brevetabilité : Condition permettant de protéger une invention par brevet, fondée notamment sur les critères de nouveauté, d'activité inventive et d'application industrielle. Toute divulgation publique préalable peut faire perdre le caractère de nouveauté et compromettre définitivement la protection. (Base légale : Code de la propriété intellectuelle (Livre VI)).

Changement substantiel de traitement : Modification affectant la finalité, les catégories de données, les destinataires, le prestataire, les modalités techniques (dont l'ajout d'un module d'IA), les transferts internationaux ou la durée de conservation, susceptible d'avoir un impact sur les droits et libertés des personnes. (Bases légales : articles 5, 13–14, 30 et 35 RGPD).

Contrôle humain effectif / Intervention humaine effective :Principe selon lequel le recours à un système d'intelligence artificielle ne dispense pas d'une supervision humaine réelle, compétente et substantielle. L'intervention humaine suppose la capacité d'analyser les éléments pertinents pris en compte par le système, d'examiner le résultat produit, de le contester et, le cas échéant, de le modifier. Une validation purement formelle ne suffit pas lorsqu'un effet académique significatif est en jeu. (Bases juridiques : article 22 RGPD ; article 14 AI Act).

Co-responsables de traitement : Entités déterminant conjointement les finalités et les moyens d'un traitement de données personnelles. (Base légale : article 26 RGPD).

Décision exclusivement automatisée : Décision produisant des effets juridiques ou affectant de manière significative une personne et reposant uniquement sur un traitement automatisé, sans intervention humaine substantielle. (Base légale : article 22 RGPD.

Déployeur (au sens du règlement européen sur l'IA) :

Personne physique ou morale utilisant un système d'intelligence artificielle sous son autorité, dans un cadre professionnel.Dans un établissement d'enseignement supérieur, l'établissement est en principe déployeur des systèmes intégrés à son organisation, tandis qu'un enseignant peut être déployeur à titre individuel lorsqu'il recourt à une IA externe dans l'exercice de ses fonctions. (Base juridique : article 3 du règlement européen sur l'IA (AI Act)).

Divulgation : Communication d'une information à un tiers non autorisé. En matière de brevet, toute divulgation non maîtrisée avant dépôt peut faire perdre la nouveauté de l'invention. En matière contractuelle, elle peut constituer une violation d'une clause de confidentialité.

Donnée à caractère personnel : toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;. (Base légale : article 4 §1 RGPD).

Données sensibles (catégories particulières de données) : Données révélant notamment l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance

syndicale, les données génétiques, biométriques, de santé ou relatives à la vie sexuelle. Ces données bénéficient d'un régime de protection renforcé. Base légale : article 9 RGPD.

Données anonymisées : Données ayant été transformées de manière irréversible de sorte qu'aucune personne physique ne puisse être identifiée par des moyens raisonnablement susceptibles d'être utilisés. Les données véritablement anonymisées sortent du champ d'application du RGPD. (Référence : considérant 26 RGPD).

Données pseudonymisées : Données personnelles traitées de telle manière qu'elles ne puissent plus être attribuées à une personne spécifique sans informations supplémentaires conservées séparément. Elles demeurent des données personnelles au sens du RGPD. (Base légale : article 4 §5 RGPD).

Données mixtes : Ensemble de données combinant des éléments scientifiques (résultats, protocoles, analyses) et des données à caractère personnel identifiables ou indirectement identifiables. Elles requièrent une double analyse : scientifique (valorisation, confidentialité) et réglementaire (RGPD).

Données contractuellement protégées : Données soumises à des engagements juridiques limitant leur communication ou leur usage, notamment dans le cadre de conventions de recherche, d'accords de consortium, de partenariats industriels ou d'accords de confidentialité (NDA). (Base légale : Code civil, articles 1101 et suivants).

Données publiques (usage en intelligence artificielle) : Les données publiques désignent des informations légalement accessibles au public, soit parce qu'elles sont communicables et réutilisables au titre du droit d'accès aux documents administratifs, soit parce qu'elles ont été rendues accessibles sans restriction technique ou juridique.

En matière d'intelligence artificielle, leur utilisation demeure subordonnée au respect des règles relatives à la protection des données personnelles et aux droits de propriété intellectuelle.

Le caractère « public » d'une donnée n'implique pas sa libre exploitation pour l'entraînement ou le fonctionnement d'un système d'IA. Sa réutilisation doit respecter les règles d'accès et de réutilisation des informations publiques ; les exigences du droit des données personnelles ; les droits d'auteur et droits voisins ; les obligations spécifiques applicables aux systèmes d'IA.

(Bases légales principales : (Code des relations entre le public et l'administration, art. L300-1 et s. (droit d'accès) ; art. L321-1 et s. (réutilisation des informations publiques) ; Règlement général sur la protection des données, art. 4, 6 et 14 (traitement de données personnelles) ; Code de la propriété intellectuelle, art. L122-5 et L342-3 (exceptions et fouille de textes et de données) ; AI Act (transparence et respect du droit d'auteur pour les modèles d'IA à usage général))

Données sensibles (catégories particulières de données) : Au sens de l'article 9 §1 du Règlement général sur la protection des données, constituent des *catégories particulières de données* (dites « données sensibles ») les données à caractère personnel qui révèlent de : l'origine raciale ou ethnique ; les opinions politiques ; les convictions religieuses ou philosophiques ; l'appartenance syndicale ; les données génétiques ; les données biométriques aux fins d'identifier une personne de manière unique ; les données concernant la santé ;les données concernant la vie sexuelle ou l'orientation sexuelle.

Leur traitement est en principe interdit, sauf si l'une des exceptions prévues à l'article 9 §2 du RGPD s'applique (notamment consentement explicite, obligation légale, intérêt public important, médecine, recherche scientifique, etc.). (bases légales : Articles 4 §13 à §15 et 9 du RGPD).

Données stratégiques : Informations dont la divulgation pourrait porter atteinte aux intérêts scientifiques, économiques, financiers ou institutionnels de l'établissement.

DPO (Délégué à la protection des données) : Personne désignée pour veiller à la conformité des traitements de données personnelles et conseiller l'établissement en matière de protection des données. (Bases légales : articles 37 à 39 RGPD).

Évaluation académique assistée par IA : Usage d'un système d'intelligence artificielle pour assister l'enseignant dans l'analyse d'une production étudiante (correction, annotation, suggestion), sans se substituer à la décision humaine finale.

Finalité du traitement : Objectif déterminé, explicite et légitime poursuivi par le traitement de données personnelles. Toute modification substantielle de finalité nécessite une nouvelle analyse de conformité. (Base légale : article 5 §1 b) RGPD).

Fournisseur (au sens du règlement européen sur l'IA) : Personne physique ou morale développant un système d'intelligence artificielle ou le faisant développer en vue de le mettre sur le marché ou de le mettre en service sous son propre nom. (Base juridique : article 3 AI Act).

Gouvernance des données : Ensemble des règles, procédures, responsabilités et mécanismes internes encadrant la gestion, la protection, la circulation, la conservation et la sécurisation des données au sein de l'établissement.

Intelligence artificielle (IA) : Au sens de l'article 3 du AI Act, un *système d'intelligence artificielle* est : « un système automatisé conçu pour fonctionner à différents niveaux d'autonomie et pouvant faire preuve d'adaptabilité après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des données d'entrée qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions susceptibles d'influencer des environnements physiques ou virtuels.

La définition est fonctionnelle et technologique-neutre. Elle couvre notamment les systèmes d'apprentissage automatique (machine learning), les modèles génératifs, et d'autres approches statistiques ou logiques produisant des résultats influençant un environnement

IA Act ou RIA : Règlement européen établissant un cadre harmonisé applicable aux systèmes d'intelligence artificielle dans l'Union européenne. Il adopte une approche fondée sur le niveau de risque

des systèmes d'IA. Il s'applique aux fournisseurs, déployeurs, importateurs et distributeurs de systèmes d'IA. Il distingue quatre niveaux : risque inacceptable, haut risque, risque limité et risque minimal. :

- Les systèmes à risque inacceptable (ex. manipulation subliminale, notation sociale étatique) sont interdits.
- Les systèmes à haut risque (éducation, emploi, justice, infrastructures critiques, santé) sont autorisés mais strictement encadrés. Ces systèmes doivent respecter des exigences de gestion des risques et de qualité des données. Ils doivent prévoir une supervision humaine effective. Une documentation technique et une évaluation de conformité sont obligatoires.
- Les systèmes à risque limité sont soumis à des obligations de transparence (ex.: obligation d'informer l'utilisateur qu'il interagit avec un chatbot ou qu'un contenu est généré par IA. information sur l'usage d'un chatbot).
- Les systèmes à risque minimal – usage libre (correcteur automatique non décisif, outil d'aide à la rédaction sans impact sur la décision académique formelle).

Les modèles d'IA à usage général (GPAI), dont les IA génératives, font l'objet d'obligations spécifiques. Les modèles présentant un risque systémique sont soumis à des exigences renforcées. Le règlement prévoit des mécanismes de surveillance par les autorités nationales compétentes. Des sanctions administratives importantes sont prévues en cas de non-conformité.

L'objectif du AI Act est d'assurer un développement de l'IA respectueux des droits fondamentaux, de la sécurité et du marché intérieur européen.

IA externe : Service d'intelligence artificielle fourni par un prestataire tiers dont l'établissement ne maîtrise ni l'infrastructure technique, ni l'hébergement, ni les modalités de réutilisation des données transmises.

IA générative : 'IA générative désigne un système d'intelligence artificielle capable de produire de nouveaux contenus (texte, images, audio, vidéo, code, etc.) à partir de données d'entrée, généralement entraîné sur de vastes ensembles de données.

Au sens du AI Act, ces systèmes relèvent le plus souvent de la catégorie des modèles d'IA à usage général (GPAI) lorsqu'ils présentent une généralité significative et peuvent être intégrés dans une pluralité d'applications en aval.

Caractéristiques juridiques principales : Production autonome de contenu (génération probabiliste) ; Entraînement sur de grands volumes de données ;Possibilité d'intégration dans divers services ou outils ;Risques spécifiques en matière de désinformation, biais, atteinte aux droits d'auteur et aux données personnelles.

(Base légale :AI Act (obligations de transparence, documentation des données d'entraînement, respect du droit d'auteur) ; Règlement général sur la protection des données si des données personnelles sont traitées ; Code de la propriété intellectuelle (protection des œuvres, fouille de textes et de données)).

Exemples d'usage: assistant de rédaction ; génération de supports pédagogiques ; aide à la programmation ; production automatisée de synthèses ou de quiz.

IA à haut risque

Catégorie prévue par le AI Act (annexes I à III). Ces systèmes sont soumis à des obligations renforcées (évaluation de conformité, gestion des risques, documentation, supervision humaine, etc.) en raison de leur impact potentiel sur la sécurité ou les droits fondamentaux.

Dans le contexte universitaire, cela concerne surtout :

1.Accès à l'éducation et sélection des étudiants

Est à haut risque une IA utilisée pour : l'admission des étudiants ; la sélection pour une formation ; l'orientation académique déterminante ; l'attribution automatisée de bourses si elle conditionne l'accès à l'enseignement.

2 Évaluation des étudiants

Est également à haut risque une IA qui : évalue les performances académiques, corrige automatiquement des examens, décide de la validation d'un diplôme, détecte la fraude si cela a un impact significatif.

3 Recrutement du personnel universitaire

Une IA utilisée pour : présélectionner des candidats enseignants-chercheurs, évaluer les candidatures à un poste, classer automatiquement les dossiers, relève aussi des systèmes à haut risque (catégorie emploi et accès à l'emploi).

4 Ce qui n'est généralement PAS à haut risque

Dans une université : un chatbot administratif, un correcteur orthographique, un outil d'aide à la rédaction, un système de recommandation de ressources pédagogiques non décisif→ ne sont pas en principe qualifiés de haut risque.

Si le système est qualifié de haut risque, l'université doit notamment : mettre en place un système de gestion des risques, assurer une documentation technique, garantir la supervision humaine, assurer la qualité des données, procéder à une évaluation de conformité, tenir un enregistrement des activités.

Intelligence artificielle générale (IAG) (pas encore de définition juridique donc approche doctrinale)
L'intelligence artificielle générale (IAG) désigne un système d'IA hypothétique capable d'accomplir, de manière autonome et polyvalente, l'ensemble des tâches cognitives qu'un être humain peut réaliser, avec un niveau comparable d'adaptabilité, de raisonnement et de compréhension interdisciplinaire.

Intégration au système d'information : Connexion technique d'un système d'IA aux infrastructures numériques de l'établissement (authentification, bases de données, ENT, Moodle, etc.), susceptible d'avoir un impact en matière de sécurité et de protection des données.

Localisation des données : Lieu géographique d'hébergement et de traitement des données. Certaines conventions ou exigences réglementaires peuvent imposer une localisation dans l'Union européenne ou dans un État offrant un niveau de protection adéquat.

Minimisation des données : Principe selon lequel seules les données strictement nécessaires à la finalité poursuivie doivent être traitées ou transmises. (Base légale : article 5 §1 c) RGPD).

Moodle (ou plateforme pédagogique institutionnelle) : Environnement numérique d'apprentissage opéré sous la responsabilité de l'établissement, pouvant intégrer des modules d'automatisation ou

d'assistance sans nécessairement constituer un système d'intelligence artificielle au sens du règlement européen.

NDA (Non-Disclosure Agreement) : Accord contractuel de confidentialité encadrant la communication et l'utilisation d'informations protégées entre des parties.

Proportionnalité : Principe selon lequel le niveau d'encadrement, de contrôle ou de restriction doit être adapté au niveau de risque identifié, sans excéder ce qui est nécessaire à la protection des droits et des intérêts en jeu.

Recherche impliquant la personne humaine (RIPH) : Recherche comportant une intervention sur une personne non justifiée par sa prise en charge habituelle et soumise à un encadrement éthique et réglementaire spécifique (avis d'un comité de protection des personnes, autorisation de l'autorité compétente selon les cas). L'usage d'un système d'intelligence artificielle dans ce contexte doit respecter à la fois le protocole validé, le RGPD et les règles de confidentialité scientifique. (Base légale : Code de la santé publique).

Responsable de traitement : Personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ; (Base légale : article 4 §7 RGPD).

Secret scientifique : Ensemble des informations de recherche non publiées dont la divulgation pourrait compromettre la stratégie scientifique, la compétitivité académique, la reconnaissance de la paternité des travaux ou la valorisation ultérieure des résultats.Il s'agit d'une notion issue des pratiques académiques et de la protection des résultats, distincte mais parfois articulée avec le secret des affaires.

Secret des affaires : Information non publique présentant une valeur économique ou stratégique, faisant l'objet de mesures raisonnables de protection et dont la divulgation est susceptible de porter atteinte aux intérêts légitimes de son détenteur. (Base légale : Directive (UE) 2016/943 ; Code de commerce, articles L151-1 et suivants).

Sous-traitant : Personne physique ou morale traitant des données personnelles pour le compte d'un responsable de traitement, conformément à ses instructions. Le recours à une IA externe peut placer le prestataire dans la position de sous-traitant au sens du RGPD. (Base légale : article 4 §8 RGPD).

Souveraineté des données : Capacité d'un établissement à conserver la maîtrise juridique et technique de l'accès, de l'usage, du stockage, de la localisation et des conditions de réutilisation de ses données.

Elle implique notamment une vigilance quant aux transferts internationaux et aux conditions contractuelles des prestataires.

Traçabilité : Capacité à documenter les traitements effectués, les finalités poursuivies, les catégories de données concernées, les acteurs impliqués et les décisions prises dans le cadre de l'usage d'un système d'intelligence artificielle. La traçabilité contribue à la transparence, à la conformité réglementaire et à la sécurité juridique.

Traitement automatisé de données : Notion issue du Règlement général sur la protection des données (art. 4 et 22).Désigne toute opération effectuée par des procédés automatisés sur des données à caractère personnel, notamment lorsqu'elle produit des effets juridiques ou affecte significativement une personne.

Traitement de données : (Article 4 RGPD) – Aux fins du présent règlement, on entend par :…2) « traitement », toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ;

Transfert international de données : Communication ou mise à disposition de données personnelles vers un pays situé en dehors de l'Union européenne ou de l'Espace économique européen. Un tel transfert est soumis à des conditions spécifiques (décision d'adéquation, garanties appropriées, clauses contractuelles types, etc.). (Bases légales : articles 44 à 49 RGPD).

Valorisation : Ensemble des actions visant à protéger, transférer et exploiter les résultats de la recherche (brevets, logiciels, bases de données, partenariats industriels, licences), dans le respect des exigences juridiques et stratégiques. Toute divulgation non maîtrisée avant protection peut compromettre la valorisation.

Science ouverte : Politique visant à rendre accessibles les publications et, lorsque cela est possible et juridiquement compatible, les données de recherche. Elle s'exerce dans le respect :

- des obligations contractuelles ;
- du RGPD ;
- des règles de propriété intellectuelle ;
- des stratégies de valorisation ;
- et de la protection du secret scientifique ou du secret des affaires.

Système d'IA à usage général (GPAI) Selon le AI Act, il s'agit d'un modèle d'IA entraîné sur de grandes quantités de données, présentant une généralité significative et pouvant être intégré dans une pluralité de systèmes en aval.

PROJET CHARTE DE L'UNIVERSITE PARIS-EST CRETEIL SUR LE BON USAGE DE L'INTELLIGENCE ARTIFICIELLE

Vendredi 13 février 2026

UPEC
Connaissance - Action
UNIVERSITÉ
PARIS-EST CRÉTEIL
VAL DE MARNE

Projet porté par
Monsieur Gaétan HAINS
Vice-Président du numérique

Monsieur Grégory QUIQUEMPOIS
Chargé de mission IA - UPEC
Professeur de SVT à l'INSPE
Chargé de mission CPC (Culture professionnelle commune)
Chargé de mission Numérique Éducatif – Référent PIX+Edu

Monsieur Pierre VALARCHER
ex Chargé de mission IA

Madame Odile DEMAZY,
Chargée de mission impacts juridiques de l'IA
environnement et contexte de travail

UPEC
Connaissance - Action
UNIVERSITÉ
PARIS-EST CRÉTEIL
VAL DE MARNE

PARTIE 1 — UNE CHARTE ISSUE D'UNE DEMARCHE STRUCTUREE, CONCERTEE ET PROFONDEMENT HUMANISTE

POURQUOI UNE CHARTE IA ?
(CONTEXTE INSTITUTIONNEL ET STRATÉGIQUE)

- **Le constat l'explosion des usages IA (étudiants, enseignants, administratifs).**
- **Des Risques systémiques :** fraude, données sensibles, décisions automatisées, altération de la recherche, surcharge organisationnelle.
- **Obligation institutionnelle d'encadrement (RGPD, AI Act, Code de l'éducation).**
- **Nécessité d'un cadre commun, protecteur et opérationnel.**

UNE CHARTE OUTIL DE CADRAGE EVOLUTIF ET PROTECTEUR

La Charte est :	La Charte n'est pas :
un outil de protection,	Il ne s'agit pas d'un catalogue d'autorisations/interdictions
un outil d'accompagnement	Un outil disciplinaire
Un outil de clarification	Un document technique réservé aux experts

Cette charte comporte des exigences exprimées sous la forme d'obligations et d'interdictions.

➢ Une Charte non exhaustive, évolutive

- Document "**cadre" commun, lisible et sécurisant pour tous les usages** d'IA au sein de l'Université.
- Elle clarifie ce qui est possible, ce qui est **encadré et ce qui est interdit, au regard des textes légaux et des exigences éthiques du service public.**
- la charte sera complétée de guides métiers, fiches réflexes,

➢ Déclinaisons

- procédures internes, **soutenue par des formations, un accompagnement**
- **Révision régulière** : comité de suivi, veille juridique/technique

UNE CHARTE ALIGNÉE SUR LES EXIGENCES RÉGLEMENTAIRES ET SCIENTIFIQUES

- **Les travaux du CEDIS et de la Commission des statuts ont confirmé la solidité juridique du cadre proposé et son articulation cohérente avec le corpus normatif existant.**

- **La rédaction de la Charte s'est appuyée sur une analyse approfondie des principaux cadres juridiques européens et nationaux :**
  - le Règlement général sur la protection des données (RGPD),
  - le Règlement européen établissant des règles harmonisées concernant l'intelligence artificielle (AI Act),
  - le Code de l'éducation, ainsi que les référentiels de cybersécurité tels que la directive NIS2 et le Cybersecurity Act, sans oublier les règles applicables au service public et les principes d'intégrité scientifique.

L'objectif a été de transformer ces normes, souvent techniques et complexes, en règles claires, compréhensibles et directement opérationnelles pour l'ensemble des membres de l'Université.

UNE CHARTE ALIGNÉE SUR LES EXIGENCES RÉGLEMENTAIRES ET SCIENTIFIQUES

- **La Charte rappelle explicitement les missions du service public de l'enseignement supérieur définies à l'article L.123-2 du Code de l'éducation et mentionne les libertés académiques**
  - (liberté d'enseignement, de recherche, d'expression académique et indépendance scientifique). Elle ne constitue pas une restriction de l'autonomie pédagogique ou scientifique mais un cadre de sécurisation des pratiques.
  - Des références explicites aux articles L.123-4-2, L.123-2, L.123-3, L123-4-1 et L123-4-2 Code de l'éducation ont été intégrées afin d'affirmer la dimension inclusive du texte et de reconnaître que l'IA peut constituer un levier d'accessibilité, sous réserve d'un encadrement éthique et sécurisé.

- **Cette démarche a été complétée par un benchmarking des chartes publiées par d'autres universités.**

UNE CHARTE S'INSCRIVANT DANS LE CADRE D'UNE DÉMARCHE COLLECTIVE ET CONSENSUELLE 2/2

- Le processus d'élaboration a été prolongé par un examen approfondi en instances (CEDIS , Commission des statuts, Comité social d'administration (CSA)), garantissant la continuité du dialogue institutionnel.

- Ces instances ont chacune donné un avis favorable à ce projet.

UNE GOUVERNANCE DÉDIÉE POUR UNE TRANSFORMATION DURABLE ET RESPONSABLE

- **La Charte prévoit la création d'un Comité de Suivi de l'IA, rassemblant les expertises technique, juridique, éthique et métier,**
  - suit les usages,
  - analyse les risques,
  - soutient les projets innovants,
  - veille à la conformité,
  - propose des mises à jour,
  - dans le respect des compétences institutionnelles .
- **Il inscrit l'Université dans une dynamique d'amélioration continue, garante de confiance, de cohérence et de responsabilité.**

1.2 UNE CHARTE FONDEE SUR DES VALEURS HUMANISTES, INCLUSIVES ET RESPONSABLES 1/2

La Charte s'appuie sur **huit valeurs fondamentales** et structurantes :

- **La curiosité et la recherche de l'innovation et de la création,** en s'appuyant sur **l'intérêt et l'engagement des utilisateurs** ;
- **La transparence**, en s'assurant que les processus mis en œuvre et les **résultats** obtenus sont **compréhensibles** ;
- **La confidentialité,** notamment des **données à caractère personnel** et des informations constituant **le patrimoine informationnel de l'Université** ;
- **L'éthique, l'intégrité scientifique, la déontologie et le respect du principe de licéité ;**
- **La prudence,** en encadrant certaines actions **pour se prémunir de conséquences indésirables ;**

1.2 UNE CHARTE FONDEE SUR DES VALEURS HUMANISTES, INCLUSIVES ET RESPONSABLES 2/2

- **L'évitement, en refusant certains usages pouvant avoir des conséquences inacceptables (contraires aux lois, à la réglementation en vigueur ou aux bonnes mœurs) ;**
- **La parcimonie et la sobriété, afin de minimiser l'impact environnemental de ces outils ;**
- **La traçabilité, en documentant et déclarant tout usage.**

Ces valeurs instaurent **une culture commune :** elles garantissent la protection des personnes, **encouragent une responsabilité partagée**, et renforcent un climat de confiance favorable à l'innovation et à l'évolution des pratiques.

La Charte vise ainsi à encadrer l'usage de l'IA sans freiner la créativité, **dans un esprit de bienveillance et de juste accompagnement,** afin que chaque membre de la communauté puisse progresser et s'approprier ces outils avec discernement.

PARTIE 2 : GLOSE DES ARTICLES DE LA CHARTE

ARTICLE 1/3 : EXIGENCES POUR L'UTILISATEUR D'UNE IA

- **Usage raisonné : l'IA ne remplace jamais le travail intellectuel.**
- **Vérification systématique des contenus (biais, erreurs, hallucinations).**
- **Protection stricte des données sensibles et personnelles.**
- **Principe général d'usage des systèmes d'IA (cf, tableau synoptique suivant)**
  - ❖L'usage des systèmes d'intelligence artificielle est apprécié au cas par cas, au regard :
  - ❖de la sensibilité des données traitées ;de la finalité poursuivie (enseignement, évaluation, recherche, gestion…) ;des effets potentiels sur les personnes et l'institution.
  - ❖Il repose sur un principe de graduation des risques
  - ❖"feu tricolore", indépendamment de toute validation générale des outils, dont les conditions d'utilisation et de traitement des données sont évolutives.

En toute hypothèse, l'utilisateur demeure tenu de respecter l'article 1.5 de la Charte.

ARTICLE 2/3 : EXIGENCES POUR L'UTILISATEUR D'UNE IA

➢Principes fondamentaux

❖**Le niveau de risque dépend de la nature des données traitées et des effets produits et non de l'outil lui-même.**

❖ **Utiliser les outils validés par l'Université.**

- Pour usages pro à enjeux (données sensibles, impacts personnes, décisions) outils université ou pré-conformes (RGPD, AI Act, sécurité, contrats).

❖ **Saisine institutionnelle requise pour pré-conformité RGPD et RIA**

Usages à risque élevé (évaluation,

- Notation – Certification – Orientation
- Gestion RH, financière, médicale ou sociale
- Suivi individualisé des étudiants ou personnels

❖**En cas de doute : s'abstenir et solliciter un avis institutionnel préalable.**

- Saisine DPO (question données)/RSSI (question sécurité système)/COSUI
- (questions à enjeux transversaux et/ou structurants).

❖**Sobriété numérique (recommandation d'évitement et de frugalité) et autonomie intellectuelle ,**

ARTICLE 3/3 : EXIGENCES POUR L'UTILISATEUR D'UNE IA

● USAGES INTERDITS	◍ USAGES TOLÉRÉS (responsabilité individuelle)	◍ USAGES RECOMMANDÉS (cadre institutionnel)
Définition : Traitement via IA non encadrée (notamment grand public / gratuite) de données protégées ou stratégiques.	Définition : Usage non critique, sans impact décisionnel, portant uniquement sur données publiques ou anonymisées.	Définition : Usage professionnel impliquant données sensibles ou impact significatif sur les personnes ou l'institution.
Données concernées : · Données personnelles (noms, notes, emails…) · Données sensibles (santé, handicap, RH…) · Données confidentielles ou stratégiques (finances, disciplinaire, sécurité SI) · Recherche non publiée / sous NDA	Conditions impératives : · Données publiques OU anonymisées (sans ré-identification possible) · Aucun effet décisionnel (note, validation, orientation, sanction) · Ne se substitue pas au jugement humain · Vérification critique obligatoire	Conditions : · Outils mis à disposition ou validés par l'Université · Conformité RGPD & AI Act · Encadrement contractuel et sécurité SI · Possibilité de saisine DPO / RSSI / COSUI
Exemples (interdits) : **✗ Transmettre des copies d'examen à une IA grand public** **✗ Analyser des notes ou listes d'étudiants via un outil externe** **✗ Soumettre des résultats de recherche non publiés**	Exemples (tolérés) : ✓ Reformuler un support de cours déjà publié ✓ Générer des QCM d'entraînement ✓ Résumer un texte réglementaire ou scientifique public	Exemples (recommandés) : ✓ Analyse pédagogique structurante ✓ Traitement RH ou financier assisté par IA institutionnelle ✓ Outils d'accompagnement étudiant validés

ARTICLE 2 EXIGENCES POUR LA CONCEPTION OU LE DÉPLOIEMENT D'UNE IA

- Transparence, confidentialité et éthique au cœur de la conception.
- Analyse d'impact obligatoire pour tout usage à haut risque.
- Supervision humaine indispensable et permanente.
- Sécurisation et cloisonnement des données d'entraînement.
- Respect strict des interdictions du Règlement IA.

ARTICLE 2 EXIGENCES POUR LA CONCEPTION OU LE DÉPLOIEMENT D'UNE IA

Haut risque en éducation/formation - Rappel : systèmes influençant décisions d'accès/évaluation/orientation peuvent être haut risque.

- **Distinction :**
  - **Usages d'assistance (risque limité) : autorisés si pas d'effet décisionnel + vérification humaine.**
  - **Usages décisionnels (haut risque) : supervision humaine effective, pas de décision exclusivement automatisée (RGPD art. 22), analyses d'impact, encadrement institutionnel.**
- **Saisines :**
  - DPO obligatoire si données personnelles ou évaluation certificative.
  - RSSI si outil externe/traitement sensible, questions sécurité/souveraineté.
  - COSUI si haut risque ou enjeux éthiques/pédagogiques/institutionnels ou au format guichet unique
  - Obligation de déploiement : supervision, gestion des risques, traçabilité, conformité AI Act.

ARTICLE 3 : EXIGENCES POUR LA PÉDAGOGIE ET DE LA FORMATION

- L'enseignant reste maître du cadre pédagogique.
- L'IA comme appui, jamais comme substitution.
- Information claire des étudiants sur les règles d'usage.
- Développement de l'esprit critique face aux outils.
- Continuité de l'enseignement même sans IA

ARTICLE 3 : EXIGENCES POUR LA PÉDAGOGIE ET DE LA FORMATION . Distinction structurante des usages

- La Charte distingue explicitement :
  - **les usages d'assistance pédagogique,** en principe à risque limité, autorisés sous réserve d'une vérification humaine . ;
  - **les usages à portée décisionnelle** (notation, validation, orientation), qualifiés d'usages à haut risque, appelant un encadrement institutionnel renforcé.

Cette distinction permet une application proportionnée du règlement européen sur l'intelligence artificielle (AI Act).

ARTICLE 4 : EXIGENCES POUR LES ÉVALUATIONS DES TRAVAUX DES ÉTUDIANTS

- **Évaluation via IA = usage à haut risque.**
- **Transparence : étudiants informés de l'usage.**
- **Traçabilité complète : audit possible.**
- **Supervision humaine obligatoire.**
- **Encadrement de la fraude et des outils de détection**
  - **Les outils de détection de contenus générés par intelligence artificielle ne constituent qu'un indice ou un élément d'alerte**, et ne peuvent, à eux seuls, constituer une preuve suffisante de fraude.
  - notamment la capacité de l'étudiant à expliquer, justifier et maîtriser son travail
  - **caractérisation d'une fraude repose sur des critères pédagogiques objectivables**, raisonnement, sa méthodologie et le contenu de sa production.

Toute procédure disciplinaire s'inscrit dans le respect du principe du contradictoire et des droits de la défense.

ARTICLE 5 EXIGENCES GÉNÉRALES ET SPÉCIFIQUES EN MATIÈRE D'USAGE DE L'IA DANS LA RECHERCHE

- Protection absolue des données scientifiques sensibles.
- Interdiction de créer ou falsifier des données via IA.
- Obligation de déclarer l'usage de l'IA dans les travaux.
- Journal d'usage détaillant prompts et corrections.

- **Traçabilité obligatoire mais proportionnée des usages de l'Iag**
  - la mention explicite de l'usage de l'IA générative (Iag) est obligatoire dans la méthodologie des travaux scientifiques lorsque celui-ci a contribué de manière substantielle ;
  - la capacité de justification a posteriori, lorsque cela est nécessaire et proportionné au regard de la nature du travail ;
  - Cette approche vise à garantir l'intégrité scientifique sans créer de charge administrative excessive.

- **L'IA ne remplace pas l'analyse scientifique.**

ARTICLE 6 : EXIGENCES POUR LA GESTION ADMINISTRATIVE (GÉNÉRALE, RH, FINANCIÈRE, SOCIALE ET/OU MÉDICALE)

- Confidentialité et neutralité du service public.
- Interdiction d'utiliser l'IA pour évaluer des agents.
- Données RH, financières et sociales strictement protégées.
- Outils validés uniquement, sécurité renforcée.
- L'IA comme appui administratif, jamais substitut.

ARTICLE 7 RESPONSABILITÉS ET SANCTIONS

- **Responsabilité de chaque utilisateur et concepteur**.
- **Audits** possibles par DPO, RSSI, auditeur interne.
- **Seules les dispositions explicitement identifiées comme obligatoires peuvent fonder une procédure disciplinaire**

  Afin d'éviter toute ambiguïté d'interprétation :

  - · Les formulations telles que « est tenu de », « doit », « est interdit », « est exigé » correspondent à des dispositions normatives obligatoires
  - · Les formulations telles que « peut », « est recommandé de », « est encouragé à » relèvent de bonnes pratiques à visée pédagogique

- · **Sanctions en cas de manquement.**
- · **Phase initiale : accompagnement et pédagogie.**
- · **Logique d'amélioration continue.**

ARTICLE 8. GOUVERNANCE ET RÉVISION

- **Charte évolutive et révisée régulièrement.**

- **Gouvernance dédiée : Création d'un Comité de suivi éthique & numérique-IA (COSUI) :**
  - rôle de veille, de conseil et d'évaluation ; accompagnement des projets ; respect des compétences des instances institutionnelles.
  - - Suivi, évaluation et conseil pour les projets IA.
  - · Audits institutionnels possibles.
  - · Adaptation aux évolutions technologiques et juridiques

Il ne s'agit pas d'un mécanisme de validation centralisée systématique, mais d'un outil d'appui et de cohérence institutionnelle.

ARTICLE 9. ACCOMPAGNEMENT

- Accompagnement structurant (guides, formations, fiches).
- Développement d'une culture commune de l'IA.
- Déclinaisons possibles par composante.
- Espace de veille et de partage d'expériences.
- Montée en compétences progressive.

Les dispositifs d'accompagnement ne créent pas d'obligations normatives autonomes.

Développement d'une culture commune de l'IA.
Montée en compétences progressive.

ARTICLE 10. DISPOSITIONS FINALES

➢10.1 Portée et périmètre

- La Charte s'applique à l'ensemble de la communauté universitaire dans le cadre des activités pédagogiques, scientifiques, administratives ou techniques.
- Elle complète les textes existants sans s'y substituer.

➢10.2 Articulation institutionnelle

La Charte s'articule notamment avec :

- – les statuts de l'Université ; le règlement intérieur ; la Charte du bon usage des moyens informatiques ; la PSSI ; la Politique d'intégrité scientifique.

Elle ne crée pas de normes concurrentes mais précise leur application dans le contexte de l'IA.

ARTICLE 10. DISPOSITIONS FINALES

➢10.3 Cohérence normative

- En cas de difficulté d'interprétation, il est fait application des dispositions de niveau supérieur et des règles les plus protectrices des droits fondamentaux et de la sécurité des systèmes d'information.

➢10.4 Validation et entrée en vigueur

- Adoption sous réserve de la validation des instances compétentes.
- Annexion au règlement intérieur.
- Entrée en vigueur à compter de la publication institutionnelle.

➢10.5 Dispositifs d'accompagnement

- Les dispositifs mentionnés à l'article 9 ont un rôle d'appui.
- Ils n'instaurent ni procédure déclarative systématique ni obligation nouvelle.

QUESTION À SOUMETTRE AUX ADMINISTRATEURS

Compte tenu du fait que la Charte sera annexée au règlement intérieur de l'Université, lui conférant une portée normative et une opposabilité à l'ensemble de la communauté universitaire,

En votre qualité d'administrateurs souhaitez-vous approuver l'annexion de la Charte du bon usage de l'intelligence artificielle au règlement intérieur de l'établissement, afin d'en garantir la pleine effectivité juridique et institutionnelle ?

Cette approbation engage l'Université dans une démarche claire : faire de l'intelligence artificielle un levier d'innovation encadré, conforme au droit et fidèle aux valeurs du service public de l'enseignement supérieur.