

Charte et guide pour l'utilisation de l'Intelligence Artificielle

Sommaire

1. Contexte	3
2. Pour tous les personnels et usagers.....	3
3. Règles spécifiques	4
3.1. Etudiants et étudiantes	4
3.2. Enseignants et enseignantes.....	4
3.3. La recherche	4
4. Cadre de référence général	5
4. 1. Intégrité scientifique.....	5
4. 2. Respect du droit d'auteur et de la propriété intellectuelle	5
4. 3. Sécurité des données et risques d'ingérence étrangère	5
4. 4. Protection des données personnelles et partage de responsabilités.....	6
5. Glossaire.....	7
5. 1. Données personnelles.....	7
5. 2. Données sensibles	7
5. 3. Données stratégiques	7
5. 4. Outil d'IA générative	8
5. 5. IA à haut risque	8
5. 6. IA responsable	8
5. 7. IA souveraine.....	9
5. 8. IA externe et IA non souveraine	9
6. Guide de bonnes pratiques	11
6. 1. Pour tous les personnels et usagers.....	11
6. 2. Pour les Étudiants et Étudiantes	11
6. 3. Pour les Enseignant et Enseignant es	11
6. 4. Pour la Recherche.....	12

1. Contexte

Le déploiement et l'adoption de systèmes d'Intelligence Artificielle (IA) dans la société sont une opportunité autant qu'un risque.

L'intelligence artificielle générative vient particulièrement questionner les pratiques dans l'enseignement supérieur, tout en soulevant des enjeux majeurs en matière d'impact environnemental et climatique. En effet, l'entraînement et l'utilisation de ces modèles s'accompagnent d'une consommation énergétique élevée, d'une utilisation importante d'eau pour le refroidissement des data centers, ainsi que d'une empreinte carbone significative, liée à la fois à la production d'électricité et à l'extraction des ressources nécessaires à la fabrication des infrastructures numériques.

La Rochelle Université se dote de la présente charte afin d'encadrer l'utilisation de ces technologies. Elle s'adresse à l'ensemble des usagers de La Rochelle université, qu'il s'agisse des étudiantes et étudiants ou des personnels (enseignants, enseignantes, enseignants-chercheurs, enseignantes-chercheuses, et fonctions support et soutien).

La Rochelle Université s'engage à créer un environnement où les solutions d'IA génératives sont utilisées de manière éthique, responsable, durable, transparente et bénéfique pour tous.

La charte a pour objectif de poser un cadre d'usage des outils d'IA générative au sein de l'université de La Rochelle. Elle s'accompagne d'un guide de bonnes pratiques, régulièrement mis à jour, pour une meilleure compréhension des usages possibles.

La charte s'inscrit dans le cadre de la législation applicable (Règlement Général de Protection des Données, Sécurisation et Régulation de l'Espace Numérique, Code de l'éducation) et respecte le règlement 2024/1689 du Parlement Européen et du Conseil Européen du 13 juin 2024.

2. Pour tous les personnels et usagers

Tous les utilisateurs d'outils intégrant l'IA se doivent de respecter des grands principes :

- > Les outils d'IA sont des assistants et ne sauraient se substituer au travail et à la réflexion des utilisateurs.
- > Aucune donnée personnelle et/ou sensible ne doit être envoyée dans des outils d'IA n'ayant pas été validés par l'Université. Les utilisateurs doivent être conscients qu'ils perdent la maîtrise des usages potentiels de ces données dès lors qu'elles sont utilisées pour interagir avec un modèle d'IA externe ou non souverain
- > Les personnels et usagers se doivent d'utiliser l'IA de manière responsable à plusieurs égards : ils doivent en avoir un usage mesuré au regard de l'empreinte énergétique et environnemental des outils ; Les personnels et usagers sont responsables des contenus que les IA produisent à leur demande. Les personnels et usagers se doivent d'utiliser l'IA de manière transparente : l'usage de l'IA doit être impérativement mentionné.
- > Les personnels et les usagers se doivent d'utiliser l'IA de manière critique : ils doivent avoir conscience que ces outils sont des outils de simulation d'intelligence pouvant introduire des biais et des erreurs. Les personnels et les usagers se doivent d'exercer leur propre esprit critique dans son usage.

L'établissement s'engage à accompagner et former les étudiants, les étudiantes, les personnels enseignants et personnels non-enseignants aux opportunités et risques liés à l'usage de l'IA.

3. Règles spécifiques

En complément des principes généraux, des règles spécifiques s'appliquent aux publics suivants :

3.1. Etudiants et étudiantes

L'usage de l'IA doit se faire un accord avec le règlement des études. Tout étudiant et toute étudiantes doit en prendre connaissance.

Son usage impose le respect des règles suivantes :

- > S'assurer auprès de l'enseignant ou l'enseignante du droit et de la manière d'utiliser l'IA générative spécifiquement pour le cours ou l'évaluation concernée.
- > Si autorisation, préciser et documenter l'utilisation de l'IA selon les consignes de l'enseignant ou l'enseignante.
- > L'étudiant ou l'étudiante expérimentant l'IA est responsable de ce qu'il produit avec l'aide de l'IA et veille à apporter un esprit critique à ses productions.

3.2. Enseignants et enseignantes

- > Communiquer explicitement aux étudiants et étudiantes les consignes d'usages de l'IA.
- > Mettre à disposition les consignes d'utilisation sous forme de document écrit dès le premier cours et les rendre disponibles pour la période.
- > Accompagner les étudiants et étudiantes vers un usage de l'IA raisonné et proportionné aux besoins d'apprentissage et pertinent dans leur future pratique professionnelle.
- > Adapter les critères et formats d'évaluation en fonction des utilisations autorisées de l'IA générative.
- > Les enseignants utilisant l'IA pour créer des contenus pédagogiques (cours, supports pédagogiques, exercices, quizz ou sujets de projets ou d'examen) doivent mettre en place un processus systématique de vérification par l'humain afin de garantir la cohérence, l'exactitude et l'équité des éléments produits ou évalués. Il veille aussi à l'absence d'erreurs factuelles, scientifiques ou méthodologiques, ainsi qu'à la neutralité et à l'absence de biais discriminants.

3.3. Chercheurs et chercheuses

Tout chercheur se doit de consulter la charte de déontologie, d'intégrité scientifique et de médiation. (CA 8 juillet 2024)

Extrait de la charte s'appliquant également dans le cadre de l'utilisation de l'IA :
« Les principes déontologiques et d'intégrité scientifique doivent guider l'action des agents dans l'exercice de leurs fonctions, en cohérence avec l'article L.123-6 du code de l'éducation, en vertu duquel le service public de l'enseignement supérieur « promeut des valeurs d'éthique, de responsabilité et d'exemplarité ».

- > Préserver la confidentialité et la valeur stratégique de l'information dans l'utilisation des outils qui manipulent l'IA.
 - > Vérifier si le contenu généré provient de sources existantes afin d'ajouter les références appropriées si nécessaire.
-

- > Distinguer le contenu généré par l'IA du reste du document.
- > Vérifier le cadre légal et le point de vue des revues, des éditeurs ou des financeurs concernant l'utilisation d'IA.

4. Cadre de référence général

L'utilisation des outils d'intelligence artificielle au sein de l'établissement s'inscrit pleinement dans le cadre éthique, scientifique et juridique qui régit l'ensemble de nos activités de recherche et d'enseignement. À ce titre, tout recours à l'IA doit respecter les principes et obligations rappelés ci-après.

4. 1. Intégrité scientifique

L'usage de l'IA ne saurait déroger aux exigences d'intégrité scientifique auxquelles sont soumis l'ensemble des membres de la communauté académique. En particulier, le recours à des outils d'IA génératifs expose à des risques réels de plagiat, y compris sous sa forme indirecte : la reprise, même reformulée, de contenus générés automatiquement sans mention explicite de leur origine constitue une atteinte à l'honnêteté intellectuelle. De même, l'utilisation de l'IA aux fins de falsification ou de fabrication de données, de résultats ou de références bibliographiques est assimilée à une fraude scientifique et traitée comme telle. Tout document produit avec le concours d'un outil d'IA doit le mentionner de manière transparente, conformément aux recommandations en vigueur.

4. 2. Respect du droit d'auteur et de la propriété intellectuelle

L'usage de l'IA doit s'inscrire dans le respect scrupuleux du droit d'auteur et, plus largement, de la propriété intellectuelle. Les contenus générés par des systèmes d'IA sont susceptibles d'incorporer, de reproduire ou d'adapter des œuvres protégées sans que cela soit apparent pour l'utilisateur. Il appartient à chacun de s'assurer que les productions issues de ces outils ne portent pas atteinte aux droits de tiers, qu'il s'agisse de textes, d'images, de données ou de codes informatiques. Par ailleurs, la question de la titularité des droits sur les contenus co-produits avec l'IA demeure juridiquement incertaine : les membres de l'établissement sont invités à la plus grande prudence quant à la valorisation ou à la diffusion de tels contenus.

4. 3. Sécurité des données et risques d'ingérence étrangère

L'utilisation de plateformes d'IA, pour la plupart hébergées par des acteurs extra-européens, expose l'établissement à des risques significatifs de captation de données stratégiques. Toute donnée saisie dans un outil d'IA tiers, qu'il s'agisse de résultats de recherche non publiés, de données personnelles, de données sensibles ou de propriété industrielle, est susceptible d'être collectée, traitée et exploitée dans des conditions ne satisfaisant pas aux exigences du droit européen, notamment le RGPD. Dans un contexte marqué par des tensions géopolitiques accrues et des risques documentés d'ingérence étrangère dans les milieux académiques et scientifiques, il est formellement déconseillé d'introduire dans ces outils toute information relevant du secret des affaires, de projets de recherche sensibles ou de données à caractère stratégique. Les membres de l'établissement sont invités à se conformer aux recommandations émises en la matière par les autorités nationales compétentes, notamment l'ANSSI et la direction générale de la sécurité intérieure (DGSI).

4. 4. Protection des données personnelles et partage de responsabilités

L'utilisation d'outils d'IA impliquant la transmission volontaire de données personnelles ou sensibles vers des services externes, non maîtrisés par l'établissement, est interdite en l'absence d'un cadre préalablement validé par les instances compétentes de l'établissement. Cette interdiction vise à prévenir tout traitement de données en dehors du périmètre de conformité défini par le RGPD et les politiques internes de sécurité des systèmes d'information.

Toutefois, cette exigence ne saurait faire obstacle à l'usage normal des outils professionnels mis à disposition par l'établissement, y compris lorsque ceux-ci intègrent des fonctionnalités d'IA, qu'il s'agisse de systèmes d'exploitation, de suites bureautiques ou d'autres environnements de travail fournis et configurés par l'établissement. Dans ce cadre, la responsabilité personnelle de l'agent ne peut être engagée dès lors qu'il n'a procédé à **aucune transmission volontaire** ou détournée de données vers un service externe non autorisé.

La responsabilité de la conformité réglementaire incombe en premier lieu à l'établissement, qui assume la charge du choix, de la configuration et du déploiement des outils mis à disposition, dans le respect du cadre juridique applicable, notamment le RGPD et les référentiels de sécurité en vigueur. Cette répartition claire des responsabilités a pour objet de garantir un environnement de travail numérique à la fois fonctionnel et sécurisé, sans faire peser sur les agents une charge de conformité qui excède leur périmètre d'action.

5. Glossaire

5. 1. Données personnelles

Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable. Mais, parce qu'elles concernent des personnes, celles-ci doivent en conserver la maîtrise.

Une personne physique peut être identifiée :

- > Directement (exemple : nom et prénom).
- > Indirectement (exemple : par un numéro de téléphone ou de plaque d'immatriculation, un identifiant tel que le numéro de sécurité sociale, une adresse postale ou courriel, mais aussi la voix ou l'image).

L'identification d'une personne physique peut être réalisée :

- > À partir d'une seule donnée (exemple : nom).
- > À partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour et membre de telle association).

CNIL 2026 (définition issue du RGPD)

5. 2. Données sensibles

Les données sensibles forment une catégorie particulière des données personnelles. Ce sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

CNIL 2026 (définition issue du RGPD)

5. 3. Données stratégiques

Sont qualifiées de **données stratégiques** l'ensemble des informations dont la divulgation, l'altération ou la captation par un tiers non autorisé serait susceptible de porter atteinte aux intérêts scientifiques, économiques ou institutionnels de l'établissement.

Cette catégorie recouvre notamment :

- **les données de recherche sensibles** : résultats non publiés, données brutes ou intermédiaires de projets en cours, savoir-faire et méthodes originales, notamment dans les domaines à fort enjeu de souveraineté (défense, santé, énergie, numérique, biotechnologies) ;
- **les données relevant de partenariats contractuels** : informations couvertes par des accords de confidentialité conclus avec des partenaires industriels, institutionnels ou internationaux, ainsi que tout élément lié à des projets financés sur appels à projets compétitifs (ANR, Europe, DGA, etc.) ;
- **les données à caractère économique et concurrentiel** : éléments relatifs à des dépôts de brevets en cours, à des processus de valorisation ou de transfert de technologie, ou à des négociations de partenariats stratégiques ;

- **les données institutionnelles sensibles** : informations relatives à la gouvernance, aux orientations stratégiques, aux situations individuelles de personnels ou d'étudiants dans des contextes sensibles, ainsi que tout élément susceptible d'affecter la réputation ou la sécurité de l'établissement.

La notion de données stratégiques se distingue de celle de **données personnelles**, (cf. Section 5.1) régie par le RGPD, avec laquelle elle peut néanmoins se recouper ponctuellement. Elle s'articule également avec les catégories définies par les autorités nationales compétentes, en particulier dans le cadre de la **protection du potentiel scientifique et technique de la Nation (PPST)**, dispositif réglementaire visant à prémunir les opérateurs publics de recherche contre les risques d'ingérence étrangère.

5. 4. Outil d'IA générative

On entend par outil d'IA générative tout système d'intelligence artificielle capable de produire, à partir d'une instruction formulée en langage naturel ou d'autres formes d'entrées, des contenus nouveaux tels que des textes, des images, des sons, des vidéos, des codes informatiques ou des données synthétiques. Ces systèmes reposent sur des modèles entraînés sur de vastes corpus de données et sont en mesure de simuler une production intellectuelle humaine sans pour autant garantir l'exactitude, l'originalité ou la neutralité des contenus générés.

Dans le cadre de la présente charte, cette notion englobe notamment les assistants conversationnels (de type *large language models*), les générateurs d'images ou de contenus multimodaux, ainsi que tout outil intégrant de telles fonctionnalités, qu'il soit accessible en ligne, via une application dédiée ou intégré à un environnement de travail professionnel.

L'usage de ces outils appelle une vigilance particulière quant à la fiabilité des contenus produits, au respect de la propriété intellectuelle et à la protection des données transmises dans le cadre de leur utilisation.

5. 5. IA à haut risque

La notion d'IA à haut risque est issue du règlement européen sur l'intelligence artificielle (*AI Act, règlement UE 2024/1689*), entré en vigueur en 2024. Elle désigne les systèmes d'IA dont les usages sont susceptibles de porter atteinte de manière significative à la santé, à la sécurité ou aux droits fondamentaux des personnes.

Le règlement européen soumet ces systèmes à des obligations renforcées en matière de transparence, de traçabilité, de supervision humaine et d'évaluation de conformité préalable à leur déploiement. Sont notamment concernés, dans le périmètre de l'enseignement supérieur et de la recherche, les systèmes utilisés à des fins d'évaluation des étudiants, de recrutement ou de sélection de personnels, de gestion de l'accès à des services essentiels, ou encore de surveillance biométrique.

Les membres de l'établissement sont invités à signaler tout projet de déploiement d'un tel système afin qu'une évaluation de conformité puisse être conduite par les services compétents.

5. 6. IA responsable

L'IA responsable désigne une approche du développement, du déploiement et de l'usage des systèmes d'intelligence artificielle fondée sur le respect de principes éthiques, juridiques et sociaux reconnus. Elle implique notamment que les systèmes d'IA soient conçus et utilisés de manière transparente, équitable, explicable et respectueuse des droits fondamentaux, et que leur impact sur les individus et la société fasse l'objet d'une évaluation continue.

Dans le contexte académique, l'IA responsable se traduit par l'exigence que tout recours à l'IA soit accompagné d'un regard critique sur ses résultats, d'une transparence sur son usage, et d'une attention portée aux biais potentiels qu'elle peut introduire dans les processus de recherche, d'évaluation ou d'enseignement. Elle suppose également que l'humain conserve en toutes circonstances un rôle de supervision et de décision finale, l'IA ne pouvant se substituer au jugement professionnel et à la responsabilité individuelle.

De plus, l'exploitation quotidienne de l'IA consomme massivement de l'énergie (pour alimenter les data centers) et de l'eau (pour les refroidir). Une démarche d'IA responsable suppose également d'en limiter l'usage aux cas vraiment utiles, afin de préserver les ressources et limiter son impact environnemental.

5. 7. IA souveraine

On entend par IA souveraine tout système ou infrastructure d'intelligence artificielle dont la maîtrise, technique, juridique et opérationnelle, est assurée par un acteur national ou européen, dans des conditions garantissant l'indépendance vis-à-vis de puissances étrangères et la conformité au cadre réglementaire applicable sur le territoire de l'Union européenne.

Dans le contexte des établissements d'enseignement supérieur et de recherche, la souveraineté en matière d'IA recouvre plusieurs dimensions : la localisation des données sur des infrastructures hébergées en Europe, le contrôle des conditions de traitement par des entités soumises au droit européen, et la capacité à auditer ou à interrompre le fonctionnement des systèmes utilisés. Elle constitue une réponse aux risques d'ingérence étrangère et de captation de données stratégiques identifiés par les autorités nationales, notamment dans le cadre des recommandations de l'ANSSI et du dispositif de protection du potentiel scientifique et technique de la Nation (PPST).

Le recours à des outils ou infrastructures d'IA souveraine est encouragé par l'établissement chaque fois que des alternatives crédibles existent, en particulier pour le traitement de données sensibles ou stratégiques.

5. 8. IA externe et IA non souveraine

Ces deux notions, distinctes mais complémentaires, permettent de qualifier le niveau de maîtrise qu'exerce l'établissement sur les outils d'IA utilisés dans le cadre professionnel.

Est qualifié d'**IA externe** tout système d'intelligence artificielle dont le traitement des données est opéré sur des infrastructures non gérées par l'établissement. Cette catégorie englobe l'ensemble des outils accessibles via des services tiers, qu'ils soient en ligne ou déployés sur des serveurs extérieurs, indépendamment de leur localisation géographique ou du statut juridique de l'opérateur.

Est qualifié d'**IA non souveraine** tout système d'intelligence artificielle dont le traitement des données est assuré sur des infrastructures hébergées en dehors du territoire français, ou relevant d'entités non soumises au droit français ou européen. Cette notion se distingue de celle d'IA externe en ce qu'elle introduit une dimension juridictionnelle : une IA peut être externe sans être non souveraine, dès lors qu'elle est hébergée par un opérateur établi en France et soumis au cadre réglementaire européen.

Ces deux qualifications peuvent se cumuler et appellent, dans ce cas, une vigilance accrue quant à la nature des données transmises, eu égard aux risques de captation et d'ingérence identifiés par les autorités nationales compétentes.

Seuls les outils d'IA externe et/ou non souveraine ayant fait l'objet d'une validation préalable par l'établissement peuvent être utilisés dans le cadre des activités professionnelles, d'enseignement

ou de recherche. Cette validation vise à s'assurer de leur conformité au cadre réglementaire applicable, notamment le RGPD, ainsi qu'aux exigences de sécurité des systèmes d'information de l'établissement.

6. Guide de bonnes pratiques

Ce guide propose des conseils pratiques pour une utilisation efficace, éthique, et sécurisée de l'IA au sein de notre université. Il complète la charte sur l'utilisation de l'IA générative, et propose une aide à la prise de décisions dans les usages quotidiens.

6. 1. Pour tous les personnels et usagers

- > **Sobriété d'usage** : Recourir aux outils d'IA de manière mesurée en pesant la valeur ajoutée de leur usage, afin d'en limiter l'impact environnemental. Privilégier les outils classiques moins énergivores (ex : moteur de recherche « classique ») pour les tâches simples.
- > **Esprit critique** : Considérer l'IA comme un outil d'aide et non comme une ressource principale. Analyser la cohérence, la pertinence et les limites des réponses produites, par exemple en croisant les informations avec d'autres sources.
- > **Évaluation des biais** : Rester vigilant face aux stéréotypes ou aux biais culturels que l'IA peut transmettre dans ses réponses. La manière dont vous formulez une question peut aussi biaiser l'analyse de l'IA et donc la réponse.

6. 2. Pour les étudiants et étudiantes

- > **L'IA comme tuteur pédagogique** : Sélectionner les tâches pour lesquelles vous utilisez l'IA afin de privilégier une utilisation qui nourrit la réflexion, sans s'y substituer.

Ce que vous pouvez demander à l'IA :

- Reformulation d'un concept
- Aide à la rédaction (vérifications orthographiques et grammaticales, corrections stylistiques)
- Aide à la structure d'un plan
- Planification de votre travail
- Un retour sur votre production
- Dialoguer avec l'IA pour s'entraîner au développement de compétences spécifiques comme par exemple en langues étrangères soit à l'écrit ou à l'oral
- > **Validation des sources** : Si l'IA cite une bibliographie, vérifier que chaque ouvrage ou article existe et contient les propos relevés par l'IA.
- > **Analyse critique** : Questionner activement ce que génère l'IA (faits, arguments, logique, omissions, etc.) et adapter les résultats en fonction de vos objectifs.
- > **Garder des traces** : En cas d'usage autorisé par les enseignants, conserver une trace de vos échanges avec l'IA (prompts et réponses) pour pouvoir justifier de votre cheminement si nécessaire.

6. 3. Pour les enseignant et enseignantes

- > **Communication avec les étudiants et étudiantes** : Intégrer un temps d'échange sur la manière dont vous souhaitez intégrer l'IA dans votre enseignement et les règles que vous souhaitez appliquer.

- > **Clarification des consignes** : Privilégier l'utilisation d'un système simple, comme des balises, pour indiquer les usages autorisés dans vos devoirs. (Voir Boîte à outils Moodle : <https://moodle.univ-lr.fr/2025/course/section.php?id=5866>)
- > **Adaptation des évaluations** : Identifier les évaluations qui peuvent être faussées par des usages de l'IA afin d'en adapter les modalités, en étant conscient que tous les étudiant.es n'ont pas le même accès aux outils.

6. 4. Pour les chercheurs et les chercheuses

- > **Intégrité de la relecture** : Éviter l'usage de l'IA pour évaluer ou résumer les travaux de vos pairs (peer-review) afin d'en garantir la confidentialité.
- > **Veille scientifique assistée** : Privilégier des outils d'IA spécialisés dans la recherche plutôt que des outils généralistes pour vos revues de littérature.



La Rochelle Université



univ-larochelle.fr