CHARTE D'USAGE DE L'INTELLIGENCE ARTIFICIELLE (IA)

Un cadre utile, responsable et protecteur pour l'AIES

PRINCIPE FONDAMENTAL

La confidentialité des informations concernant les personnes accompagnées, leurs familles et les professionnels prime sur tout gain de temps ou de productivité lié à l'IA. Aucune donnée permettant d'identifier directement ou indirectement une personne accompagnée ne doit être saisie dans une IA généraliste ou dans un outil non expressément validé par l'AIES.

Version	1.0
Date	Octobre 2026
Périmètre	Siège, établissements et services de l'AIES
Validation	Direction générale - après consultation du CSE et du DPO

Association pour l'Insertion l'Éducation Et les Soins
Siège social
38 Boulevard Paul Cézanne
78280 Guyancourt
Tél. 01 30 50 22 56
contact@association-ies.fr
www.association-ies.fr
CODE APE : 8610Z
SIRET : 775 706 183 00204

TABLE DES MATIÈRES

1. Objet et finalité 3
2. Champ d'application 3
3. Les six principes de l'AIES 3
4. Règle essentielle : protéger les données des personnes accompagnées 4
5. Anonymisation : une exigence réelle, pas seulement la suppression du nom 4
6. Usages autorisés de principe 4
7. Usages interdits ou soumis à validation préalable 5
8. Classification simple des données 5
9. Vérification humaine obligatoire 6
10. Écrits concernant les personnes accompagnées 6
11. Validation des outils et des nouveaux usages 6
12. Confidentialité des réunions, images et enregistrements 7
13. Ressources humaines et management 7
14. Formation et sensibilisation 7
15. Incident, erreur ou fuite de données 7
16. Responsabilités 8
17. Manquements et opposabilité 8
18. Entrée en vigueur et révision 8
ANNEXE 1 - Le réflexe AIES avant d'utiliser une IA 9
ANNEXE 2 - Exemples rapides 9
ANNEXE 3 - Documents opérationnels à tenir à jour 10
Références de conception 10

1. Objet et finalité

L'AIES reconnaît que les outils d'intelligence artificielle peuvent faciliter certaines tâches professionnelles : rédaction, synthèse, préparation de supports, recherche documentaire, mise en forme ou analyse. Leur usage doit toutefois rester compatible avec les missions de l'association, la dignité et les droits des personnes accompagnées, le secret professionnel, la confidentialité, la protection des données et la sécurité du système d'information.

La présente charte fixe les règles applicables à tout usage professionnel d'un système d'intelligence artificielle au sein de l'AIES. Elle complète le règlement intérieur, la charte informatique, les procédures RGPD, les règles de sécurité, les procédures qualité et les obligations propres à chaque métier.

L'IA est un outil d'assistance, jamais un substitut au professionnel. La décision, l'analyse d'une situation et la responsabilité restent humaines. Un résultat produit par une IA doit toujours être considéré comme un brouillon ou une aide à vérifier.

2. Champ d'application

La charte s'applique à l'ensemble des salariés, cadres, stagiaires, alternants, intérimaires, bénévoles, administrateurs lorsqu'ils utilisent des outils professionnels, prestataires et intervenants extérieurs autorisés.

Elle couvre les usages réalisés sur les équipements de l'AIES mais également tout usage professionnel réalisé depuis un équipement ou un compte personnel. L'utilisation d'un outil personnel ne permet jamais de contourner les règles de la présente charte.

3. Les six principes de l'AIES

Confidentialité d'abord : Aucune information confidentielle ou relative à une personne accompagnée ne doit être exposée à un quelconque outil.

Responsabilité humaine : Le professionnel reste responsable du contenu qu'il utilise, transmet, signe ou intègre dans un dossier.

Utilité et proportionnalité : L'IA n'est utilisée que lorsqu'elle apporte une utilité professionnelle réelle et avec le minimum de données nécessaire.

Outils validés : Un outil gratuit, une extension, un connecteur ou une fonction IA intégrée à un logiciel n'est pas utilisable du seul fait qu'il est accessible. Nous définirons au fur et à mesure la liste des outils validés.

Vérification systématique : Les résultats peuvent être inexacts, incomplets, biaisés ou inventés. Toute information diffusée doit être contrôlée.

Respect des personnes : Aucune décision individuelle concernant une personne accompagnée, un salarié ou un candidat ne peut être déléguée à une IA.

4. Règle essentielle : protéger les données des personnes accompagnées

INTERDICTION DE PRINCIPE

Dans les IA généralistes et les outils non validés par l'AIES, il est interdit de saisir, copier-coller, importer, téléverser, dicter ou faire analyser des données non anonymisées concernant une personne accompagnée, même si l'objectif est uniquement de reformuler ou de résumer un écrit.

Sont notamment concernés :

- Nom, prénom, initiales, date de naissance, adresse, photographie, voix ou tout identifiant ;
- Données de santé, handicap, diagnostic, traitement, comportement, autonomie ou vulnérabilité ;
- Projet personnalisé, compte rendu éducatif, social, psychologique ou médical, transmissions et notes de suivi ;
- Informations relatives à la famille, à la scolarité, au logement, aux ressources, à la vie affective ou sociale ;
- Faits de violence, maltraitance, harcèlement, incident grave, danger ou mesure de protection ;
- Tout ensemble de détails qui, même sans nom, permettrait de reconnaître la personne.

5. Anonymisation : une exigence réelle, pas seulement la suppression du nom

Supprimer le nom d'une personne ne suffit pas toujours. Une situation peut rester identifiable par le croisement de l'âge, de l'établissement, du handicap, de la commune, d'un événement rare ou de détails familiaux. Pour un usage autorisé avec une IA généraliste, le contenu doit être véritablement anonymisé et ne plus permettre, raisonnablement, de relier les informations à une personne.

Exemple :

À éviter : « garçon de 14 ans accueilli à l'ITEP X, scolarisé dans telle commune, ayant connu tel incident ». Préférer, si l'usage est réellement nécessaire : « adolescent accompagné en établissement médico-social », en supprimant tous les détails non indispensables.

6. Usages autorisés de principe

Sous réserve d'utiliser un outil autorisé par l'AIES et de ne transmettre aucune donnée interdite, l'IA peut notamment être utilisée pour :

- Améliorer la forme, l'orthographe ou la clarté d'un texte non confidentiel ;
- Préparer un plan, une trame de réunion, une présentation ou un support d'une intervention ;
- Résumer un document public ou un document interne non sensible ;
- Préparer un premier brouillon de courrier, procédure, fiche pratique ou communication ;
- Rechercher des idées, comparer des formulations ou vulgariser un contenu général ;
- Effectuer une recherche documentaire sur des sources ouvertes, avec vérification des sources.

7. Usages interdits ou soumis à validation préalable

Sont interdits sans validation expresse de l'AIES :

- L'utilisation d'un outil IA non validé pour traiter des informations professionnelles confidentielles ;
- L'import d'un dossier usager, d'un extrait de DUI, d'un compte rendu, d'une transmission ou d'un document comportant des données personnelles nominatives ;
- La transcription ou l'analyse par IA d'un entretien, d'une réunion ou d'un échange concernant des personnes accompagnées sans cadre validé par la Direction ;
- L'intégration automatique d'un texte généré par IA dans un dossier usager ou un écrit professionnel sans contrôle humain ;
- L'utilisation de l'IA pour décider seule d'une admission, orientation, sanction, évaluation, recrutement, évolution professionnelle ou mesure ayant un effet sur une personne ;
- L'installation d'une extension, d'un agent, d'un connecteur ou d'un module IA sur le SI de l'AIES sans autorisation ;
- L'utilisation d'un compte ou d'une messagerie personnelle pour contourner les restrictions.

8. Classification simple des données

Catégorie	Exemples	IA généraliste	Règle AIES
Publiques	Sites publics, textes officiels, données ouvertes	Oui	Vérifier les sources et les droits de réutilisation
Internes non sensibles	Trame générique, procédure sans données personnelles	Oui, avec outil autorisé	Ne pas inclure d'éléments confidentiels
Personnelles / confidentielles	Salariés, partenaires, situations internes	Non par défaut	Uniquement dans un outil et un cas d'usage expressément validés
Hautement sensibles	Usagers, santé, handicap, secret professionnel, mineurs, majeurs protégés, incidents graves	Interdit	Traitement IA uniquement dans un dispositif spécifiquement validé, sécurisé et encadré

9. Vérification humaine obligatoire

Avant d'utiliser une production issue d'une IA, l'utilisateur doit vérifier au minimum :

- L'exactitude des faits, chiffres, dates, références juridiques et sources ;
- La cohérence avec le contexte réel et les informations dont il dispose ;
- L'absence de données inventées ou de citations fictives ;
- La neutralité du ton, l'absence de stéréotype ou de formulation discriminatoire ;
- La conformité avec les règles professionnelles et les positions de l'AIES.

La personne qui transmet ou signe le document en assume le contenu. La mention « produit par l'IA » ne transfère aucune responsabilité à l'outil.

10. Écrits concernant les personnes accompagnées

Compte tenu de la sensibilité particulière des informations traitées par l'AIES, l'usage d'une IA pour produire, résumer, reformuler ou analyser un écrit relatif à une personne accompagnée est interdit dans un outil généraliste. Un tel usage ne pourra être envisagé que dans le cadre d'un outil spécifiquement validé par l'AIES, après analyse des garanties de confidentialité, de protection des données, d'hébergement, de réutilisation des données et de sécurité.

Même dans un outil validé, l'IA ne doit pas conduire à standardiser l'accompagnement ni à remplacer l'observation, l'expertise et le jugement professionnel. Les écrits engageant une appréciation clinique, éducative, sociale ou médico-sociale restent sous responsabilité humaine.

11. Validation des outils et des nouveaux usages

Tout nouvel outil, fonctionnalité, connecteur ou cas d'usage impliquant de l'IA doit être signalé avant utilisation lorsqu'il traite des données internes, personnelles ou sensibles, ou lorsqu'il s'intègre à un logiciel métier.

L'examen porte notamment sur : la finalité, les données utilisées, l'éditeur, les conditions contractuelles, l'hébergement, la réutilisation éventuelle des données, les transferts, la sécurité, les droits d'accès, la traçabilité et les risques pour les personnes.

Gouvernance proposée

Usages bureautiques à faible risque : validation dans le cadre de la liste des outils autorisés.

Usages métier ou données personnelles : instruction associant à minima la direction concernée, la fonction numérique/SI et le DPO.

Usages structurants ou à risque élevé : arbitrage de la Direction générale / CODIR.

12. Confidentialité des réunions, images et enregistrements

Les fonctions de prise de notes automatique, transcription, résumé de visioconférence, reconnaissance vocale ou analyse d'image sont des traitements à part entière. Elles ne doivent pas être activées par défaut. Leur utilisation dans une réunion, un entretien, une synthèse ou une situation impliquant des personnes accompagnées nécessite un cadre expressément validé et l'information des personnes lorsque celle-ci est requise.

Il est interdit d'utiliser une IA grand public pour analyser des photographies, vidéos ou enregistrements audio de personnes accompagnées.

13. Ressources humaines et management

L'IA peut aider à préparer des trames, des fiches de poste génériques ou des supports de management ne comportant pas de données personnelles. En revanche, les données individuelles des salariés, candidats ou professionnels ne doivent pas être saisies dans une IA généraliste.

Aucune décision de recrutement, d'évaluation, de sanction, de rémunération, d'évolution professionnelle ou d'organisation individuelle ne peut être prise automatiquement par une IA. Tout projet d'IA susceptible d'affecter l'organisation du travail ou de permettre un contrôle de l'activité doit être examiné au regard des obligations sociales applicables.

14. Formation et sensibilisation

L'AIES organise une sensibilisation générale aux usages de l'IA. L'accès à certains outils ou cas d'usage peut être conditionné à une formation ou à une habilitation spécifique. Les managers relaient les règles et s'assurent que les équipes savent identifier les informations qui ne doivent jamais être transmises à une IA.

15. Incident, erreur ou fuite de données

Tout utilisateur qui constate ou soupçonne :

- La saisie accidentelle de données confidentielles dans un outil IA ;
- Une fuite, une réutilisation inattendue ou un accès non autorisé ;
- Une erreur grave produite par une IA et susceptible d'avoir un impact sur une personne ;
- Un usage non autorisé ou le contournement d'une règle de sécurité

doit le signaler sans délai à son responsable et au canal interne désigné par l'AIES (DPO / référent SI / Direction selon la procédure en vigueur). Le signalement rapide vise d'abord à limiter les conséquences et à permettre les mesures correctrices nécessaires.

16. Responsabilités

Direction générale : fixe le cadre, valide les orientations et arbitre les usages structurants.

Directions de pôle et directions : identifient les besoins, veillent à l'application des règles et remontent les nouveaux cas d'usage.

DPO : évalue les enjeux de protection des données et la nécessité éventuelle d'une analyse d'impact.

Fonction SI / prestataires SI habilités : évalue la sécurité, l'intégration, les accès et les conditions techniques.

Qualité : articule les usages IA avec les procédures, la gestion des risques et l'amélioration continue.

Chaque utilisateur : respecte la charte, protège les données, vérifie les résultats et signale les incidents.

17. Manquements et opposabilité

Le non-respect de la présente charte peut entraîner des mesures correctrices, la suspension d'accès à certains outils et, lorsque les conditions juridiques sont réunies, les suites prévues par le règlement intérieur, les obligations professionnelles ou les engagements contractuels. La charte ne crée pas d'échelle autonome de sanctions.

Si l'AIES souhaite rendre les obligations générales et permanentes de cette charte pleinement opposables aux salariés, son articulation avec le règlement intérieur et les formalités correspondantes devront être sécurisées, notamment avec consultation du CSE.

18. Entrée en vigueur et révision

La charte entre en vigueur à la date fixée par l'AIES après accomplissement des formalités applicables. Elle est diffusée à l'ensemble des professionnels et intégrée aux actions de sensibilisation. Elle est revue au moins annuellement, ainsi qu'en cas d'évolution réglementaire, technologique ou organisationnelle significative.

ANNEXE 1 - Le réflexe AIES avant d'utiliser une IA

1. Est-ce un usage professionnel utile et légitime ?
2. L'outil figure-t-il parmi les outils autorisés par l'AIES ?
3. Mon texte, fichier, image ou audio contient-il une information sur une personne accompagnée, une famille ou un salarié ?
4. La personne pourrait-elle être reconnue indirectement, même si j'ai supprimé son nom ?
5. Ai-je réellement besoin de transmettre cette information à l'IA ?
6. Suis-je capable de vérifier le résultat produit ?
7. Le document final sera-t-il relu et assumé par un professionnel ?

EN CAS DE DOUTE : NE PAS TRANSMETTRE LA DONNÉE.

Demander conseil au manager, au DPO ou au référent SI avant d'utiliser l'outil.

ANNEXE 2 - Exemples rapides

Situation	Statut	Pourquoi
Demander à une IA de corriger un courriel institutionnel sans donnée personnelle	AUTORISABLE	Usage rédactionnel à faible risque, avec outil validé.
Copier un projet personnalisé anonymisé seulement par suppression du nom	INTERDIT	La personne peut rester identifiable et le contenu relève de l'accompagnement.
Demander une trame générique de projet personnalisé	AUTORISABLE	Aucune donnée réelle n'est transmise.
Téléverser un compte rendu d'incident concernant un usager	INTERDIT	Données hautement sensibles.
Faire résumer un texte réglementaire public	AUTORISABLE	Source ouverte, sous réserve de vérifier le résumé.
Activer un bot de transcription dans une synthèse d'équipe	VALIDATION PRÉALABLE	Risque de captation de données sensibles et de confidentialité.
Demander à l'IA de choisir entre deux candidats à partir de leurs CV	INTERDIT	Décision individuelle et données personnelles.

ANNEXE 3 - Documents opérationnels à tenir à jour

- Liste des outils IA autorisés et des comptes institutionnels à utiliser.
- Catalogue des cas d'usage autorisés et des cas soumis à validation.
- Canal de demande de validation d'un nouvel outil ou d'un nouveau cas d'usage.
- Canal de signalement d'un incident IA / données.
- Référentiel de classification des données et consignes d'anonymisation.
- Liste des formations ou habilitations requises.

Références de conception

Cette charte a été adaptée au contexte de l'AIES à partir du « Modèle de charte IA opérationnelle » transmis par l'association (avril 2026), notamment ses recommandations relatives à la responsabilité humaine, aux données hautement sensibles, à la validation des outils, à la formation, au signalement et à la gouvernance. Elle tient également compte des recommandations de la CNIL sur l'usage des IA génératives et des repères HAS/CNIL applicables aux secteurs du sanitaire, social et médico-social.

Validation Direction Générale	Avis/consultation CSE	Avis/consultation DPO
Date : 04/11/2026 Signature : 	Date : 13/10/2026	Date : 16/10/2026