Projet de règles d'usage de l'IA

Formation IA, Collège de Bonne-Espérance. Un point de départ, à compléter par l'école.

1. Les outils autorisés

Claude Entreprise, avec le compte de l'école. Pas de compte personnel ni d'outil gratuit pour des documents de l'école.

2. Les données interdites sans accord

Les données de santé des élèves (bilans logo, rapports médicaux), les dossiers DACCE, les données des parents. Ces données restent hors de portée de l'IA tant que l'école n'a pas validé.

3. Ce que l'IA ne fait jamais seule

Envoyer un message, supprimer un fichier, décider pour un élève. L'IA prépare et résume, une personne décide. Évaluer des élèves peut être un usage à haut risque au sens de l'AI Act.

4. Toujours vérifier

Les faits, les chiffres, les dates et les sources se vérifient dans le document d'origine avant tout usage. La personne qui signe reste responsable.

5. Un registre simple

Pour chaque usage régulier: quel outil, pour quoi faire, quelles données. Une page partagée suffit.

6. Le DPO valide

Le délégué à la protection des données (DPO) du pouvoir organisateur valide les usages qui touchent des données personnelles. La circulaire 9757 finance cette mission.

7. Les skills, les plugins et les connecteurs

Seulement les nôtres, ceux d'Anthropic, et ceux que l'admin a approuvés. Rien de trouvé sur Internet sans son accord: une skill ou un plugin inconnu peut cacher des instructions pour l'IA.

8. La prudence avec les agents

Ne jamais donner en même temps à un agent l'accès à des données privées, du contenu non fiable (pages web, mails reçus) et un accès à Internet. Lire chaque demande de permission avant de dire oui.

À compléter par l'école, pour éviter les problèmes d'audit

- Vérifier le contrat avec Anthropic: l'accord de traitement des données (DPA), le lieu de traitement et de stockage (États-Unis), la durée de conservation, et les modèles à éviter avec des données personnelles (Fable: 30 jours de conservation au moins).
- Choisir la base légale de chaque traitement de données personnelles (RGPD).
- Faire une analyse d'impact (AIPD) avant tout usage avec des données sensibles.
- Décider s'il faut informer les parents, et comment.
- Régler la confidentialité dans la console: désactiver l'évaluation des conversations, fixer une durée de conservation, désactiver la mémoire.
- Désigner qui tient le registre et qui le revoit, par exemple une fois par an.
- Faire valider ces règles par le pouvoir organisateur.

Ce document n'est pas un avis juridique. Il sert de base de discussion avec le pouvoir organisateur et le DPO.