



**COLLECTIF RÉGIONAL
DE DÉVELOPPEMENT**
DU BAS-SAINT-LAURENT

Politique d'utilisation de l'intelligence artificielle

**Collectif régional de développement
du Bas-Saint-Laurent**

Adoptée le 27 novembre 2025

TABLE DES MATIÈRES

	Pages
1. Objectif de la politique	4
2. Champ d'application de la politique	4
3. Champ d'utilisation.....	4
4. Limites et restrictions	5
5. Pouvoir, responsabilités et obligations des intervenant·es	6
6. Gestion des données sensibles et confidentielles	7
7. Révision de la politique	8
8. Entrée en vigueur	8

Préambule

L'intelligence artificielle (IA) est devenue un outil incontournable pour les organisations. Celle-ci vient en soutien aux opérations et apporte un avantage significatif sur des aspects stratégiques autant dans l'aide à la décision que dans l'automatisation de certaines tâches.

L'IA doit toutefois être utilisée de manière responsable et réfléchie. Celle-ci peut générer des défis en ce qui concerne notamment le respect de la confidentialité, la protection des données, les biais algorithmiques, la propriété intellectuelle, les impacts environnementaux, l'ingérence externe, l'éthique et la déontologie.

Le présent guide a pour but de baliser les pratiques d'utilisation de l'IA au sein du Collectif régional de développement du Bas-Saint-Laurent (CRD).

1. OBJECTIF DE LA POLITIQUE

- **Encadrer et promouvoir l'utilisation responsable de l'IA** pour donner aux personnes employées, élues et aux fournisseurs du CRD les balises qui favorisent :
 - L'utilisation des outils d'IA de façon à conjuguer le potentiel d'optimisation du travail avec la valorisation du savoir-faire et de l'expertise de chacun·e.
 - La compréhension des enjeux, ainsi que des questions éthiques et légales que l'utilisation de l'IA peut représenter.
- **Définir des lignes directrices claires** quant aux domaines d'application appropriés et à ses limites et restrictions.
- **Assurer la transparence et la confiance** auprès du personnel et des parties prenantes quant à l'utilisation de technologies d'IA au sein de l'organisation.
- **Protéger la confidentialité et la sécurité des données**, notamment en ce qui concerne l'information personnelle et confidentielle.
- **Fournir des orientations sur les responsabilités et rôles des utilisateurs** de l'IA.

2. CHAMP D'APPLICATION DE LA POLITIQUE

La présente politique s'applique à tous les membres du conseil d'administration du CRD ainsi qu'à ses employé·es et fournisseurs qui utilisent les outils d'intelligence artificielle, ou qui pourraient être appelés à les utiliser dans le cadre de leur travail ou mandat.

3. CHAMP D'UTILISATION

L'IA a la capacité de répondre à des besoins spécifiques et variés. Elle met en relation une multitude d'informations issues de vastes bases de connaissances et a la capacité de s'adapter à la personne utilisatrice et à ses besoins particuliers. Elle peut analyser des données complexes, générer des contenus créatifs, automatiser des tâches, améliorer les interactions professionnelles et aider à percevoir l'environnement avec plus de précision.

Toutefois, si le CRD reconnaît que l'IA comporte de nombreux avantages, celle-ci a autant de limites : elle porte des biais et ne remplace en rien l'expertise humaine. **L'IA reste un outil complémentaire** et se doit d'être limitée à un rôle d'assistance à la réalisation d'une tâche.

L'IA peut être utilisée dans les domaines suivants, sous réserve du respect des lignes directrices de cette politique :

- **Communication et rédaction** : amélioration de la rédaction formelle et informelle, génération de résumés, rédaction de procès-verbaux, synthèses, génération de tableaux, traduction, et de la personnalisation des communications de masse adapté.
- **Automatisation de tâches répétitives** : simplifier les processus administratifs (ex. : reconnaissance et tri de documents, réponses automatiques aux questions fréquemment posées).
- **Analyse de données** : identifier des tendances et prévisions dans les données, pour des prises de décisions plus rapides et éclairées.
- **Création de contenu** : aider à la production de nouveaux contenus numériques, tels des images ou des vidéos ou encore des formations personnalisées pour les employé-es.
- **Planification et résolution de problèmes** : permet de s'orienter les recherches de contenu et d'identifier des pistes de solutions à des enjeux organisationnels.

À chaque utilisation d'un outil d'IA, le ou la membre de l'équipe qui y recourt doit effectuer une révision minutieuse du contenu produit ainsi que valider les sources lorsque pertinent.

4. LIMITES ET RESTRICTIONS

Les principaux points de vigilance quant à l'utilisation de l'IA sont les suivants :

- **Éviter la dépendance excessive** : l'IA doit être utilisée pour des usages pertinents et nécessaires.
- **Transparence** : lorsque l'IA est utilisée, le ou la destinataire doit en être informé, par exemple dans les références de rapports ou dans le cas d'évaluation du personnel.
- **Consentement** : il est proscrit d'utiliser la voix, l'apparence, ou des données sensibles d'une personne sans son consentement.
- **Protection des données personnelles et des informations confidentielles** : toute utilisation de l'IA doit respecter les politiques de protection des données et les lois applicables en matière de confidentialité.
- **Responsabilité et imputabilité** : les décisions et recommandations découlant de l'IA ne réduisent pas la responsabilité des personnes utilisatrices et de l'organisation. Les

personnes utilisatrices doivent toujours valider les recommandations de l'IA et éviter les biais ou erreurs potentiels.

- **Respect des droits d'auteur·trices et de la production artistique:** l'utilisation de l'IA ne doit aucunement utiliser, transformer ou réaliser des productions artistiques ou œuvres littéraires, afin de ne pas porter atteinte aux artistes, auteur·trices et aux œuvres réelles.

5. POUVOIR, RESPONSABILITÉS ET OBLIGATIONS DES INTERVENANT·ES

Voici les rôles et les responsabilités spécifiques liés à l'utilisation de l'intelligence artificielle par les intervenant·es du CRD :

Conseil d'administration

- Adopte la présente politique.

Direction générale

- Est responsable de l'application de la politique.
- Soutient les directions de secteur et les employé·es en fournissant les ressources nécessaires pour une utilisation appropriée et efficace de l'IA.
- Fait la promotion d'une culture organisationnelle valorisant l'utilisation responsable des outils d'IA.
- Assure la mise à jour de la politique.

Direction de secteur

- Assure la diffusion et la bonne compréhension de la politique auprès de son équipe et des fournisseurs.
- Encourage une utilisation responsable de l'IA pour des tâches pertinentes et conformes aux objectifs du CRD.
- S'assure d'identifier les besoins de formation des employé·es en lien avec l'utilisation des outils d'IA.
- Signale toute utilisation inappropriée ou tout incident de sécurité lié à l'intelligence artificielle auprès de la direction générale et du responsable des technologies de l'information.

Responsable des technologies de l'information

- S'assure que les outils d'IA sont correctement configurés, sécurisés et accessibles aux utilisateurs et utilisatrices autorisés seulement (authentification, contrôle des données, audit et surveillance, gestion des vulnérabilités).
- Identifie, en collaboration avec les directions de secteur, des sessions de formation régulières pour sensibiliser les employé·es à l'utilisation appropriée des outils d'IA, à leurs impacts négatifs et à la gestion des informations sensibles.
- Soutient les directions de secteur en fournissant des conseils sur l'utilisation responsable de l'intelligence artificielle.
- Fournit une assistance technique aux utilisateurs·trices en cas de difficultés d'accès ou de problèmes lors de l'utilisation des outils d'intelligence artificielle.

Employé·es et administrateur·trices

- Utilise les outils d'IA conformément à la présente politique.
- Est responsable de ne pas injecter d'informations sensibles ou confidentielles dans les outils d'IA.
- Conserve un sens critique et s'assure de vérifier la véracité et l'exactitude des éléments générés par l'IA avant de les utiliser ou de les rendre accessibles, notamment en ce qui concerne :
 - Les biais et la discrimination que les outils d'IA peuvent générer (biais algorithmique)
 - Les erreurs et les inventions générées par l'IA (hallucination de l'IA)
 - Les erreurs et confusions sémantiques (sens et signification du langage)
- S'assure du respect de la propriété intellectuelle et de la législation dans l'utilisation des outils d'IA.
- Au besoin, informe l'utilisateur final de l'utilisation des outils d'IA pour la génération de contenu.
- Signale toute utilisation inappropriée ou tout incident de sécurité à son ou sa supérieur immédiat·e ou au service des technologies de l'information.
- Participe aux formations en lien avec l'IA proposées par l'organisation.
- S'engage à mentionner l'utilisation d'un outil IA de façon claire et explicite lorsqu'utilisée dans la production de contenu public.

6. GESTION DES DONNÉES SENSIBLES ET CONFIDENTIELLES

Lors de l'utilisation des outils d'IA, la personne utilisatrice doit pouvoir reconnaître des données sensibles et confidentielles. Elle doit aussi être en mesure d'évaluer si l'utilisation de l'outil d'IA pourrait permettre le partage d'informations sensibles et confidentielles à l'extérieur de l'organisation.

Ces informations sensibles et confidentielles sont des données qui, si elles étaient divulguées, pourraient causer des préjudices au CRD, à ses employé-es, les membres de son conseil d'administration ou à d'autres parties prenantes liées de près ou de loin au CRD (données qui permettent l'identification d'employé-es, rapports internes, données financières ou stratégiques, etc.)

Pour déterminer si une donnée est sensible ou confidentielle, la personne utilisatrice doit se poser les questions suivantes :

- Cette donnée pourrait-elle causer des préjudices si elle est divulguée?
- Cette donnée est-elle protégée par des réglementations ou des lois spécifiques?
- Cette donnée concerne-t-elle des personnes ou des entités identifiables?

La personne utilisatrice est responsable de s'informer auprès de son supérieur immédiat ou sa supérieure immédiate afin de déterminer si une donnée est sensible ou confidentielle avant de la soumettre à l'intelligence artificielle.

7. RÉVISION DE LA POLITIQUE

Compte tenu de la nouveauté et de la rapidité d'évolution de l'IA, il est convenu que cette politique doit être révisée régulièrement et que son adaptation doit être agile et proactive.

8. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur le 1^{er} décembre 2025.

Adopté le X novembre 2025

Signature de l'employé

Date

Signature de l'employeur- CRDBSL

Date