Centre
de services scolaire
des Laurentides
Québec

Code : DG-01-20-010

POLITIQUE RELATIVE À LA GOUVERNANCE DE L'INTELLIGENCE ARTIFICIELLE GÉNÉRATIVE

Unité administrative : Secrétariat général et Service informatique

13, rue Saint-Antoine
Sainte-Agathe-des-Monts (Québec) J8C 2C3
Téléphone : 819 326-0333
Télécopieur : 819 326-2121
www.csslaurentides.gouv.qc.ca

1. Préambule

L'intelligence artificielle (IA) transforme les environnements éducatifs et administratifs en offrant de nouvelles possibilités d'optimisation et d'automatisation des tâches. Toutefois, son utilisation doit être encadrée afin de garantir une approche responsable, éthique et sécurisée, alignée sur les orientations gouvernementales et les meilleures pratiques en matière de cybersécurité et de protection des renseignements personnels.

Le Centre de services scolaire des Laurentides (CSSL) reconnaît la valeur ajoutée de ces technologies tout en veillant à ce qu'elles soient utilisées de manière rigoureuse et transparente.

2. Objectifs

La Politique relative à la gouvernance de l'intelligence artificielle générative (Politique) établit les règles, rôles et contrôles encadrant l'identification, l'expérimentation, l'acquisition, l'utilisation et le déclassement des systèmes d'intelligence artificielle générative (IAG) au sein du CSSL, en conformité avec les exigences légales et gouvernementales applicables. Elle vise à :

- Encadrer l'utilisation de l'IA au sein du CSSL dans un cadre éthique et légal.
- Prévenir les risques liés à la confidentialité, la sécurité et l'intégrité des données.
- Favoriser une utilisation responsable et transparente des outils d'IA.
- Favoriser l'innovation pédagogique et administrative tout en maintenant un encadrement rigoureux.

3. Champ d'application

La politique s'applique :

- À toutes les personnes en lien avec le CSSL :
  - Les membres du personnel;
  - Les élèves inscrits dans les établissements du CSSL et leurs parents;
  - Les consultants, stagiaires et tout tiers travaillant pour ou avec le CSSL et ayant accès aux environnements numériques ou aux données de l'organisation;
  - Les partenaires externes et fournisseurs qui fournissent une solution IAG.
- À tout système d'IAG (interne, infonuagique, tiers, code, API, connecteurs) utilisé dans le cadre des fonctions du CSSL;
- À toutes les données détenues par le CSSL et aux données numériques gouvernementales.

4. Cadre légal et réglementaire

L'utilisation de l'IA doit respecter les législations et réglementations en vigueur, notamment :

- *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LGGRI) (RLRQ, c. G-1.03);
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (LAI) (RLRQ, c. A-2.1);
- *Loi concernant le cadre juridique des technologies de l'information* (RLRQ, c. C-1.1);
- *Loi sur les droits d'auteur* (LRC 1985, c. C-42)
- Ministère de la Cybersécurité et du Numérique du Québec (MCN) – *Indication d'application* (19 décembre 2025) et Énoncé de principes pour une utilisation responsable de l'intelligence artificielle par les organismes publics (gouvernance, gestion des risques, formation, critères de sélection des cas d'usage);

- Stratégie gouvernementale d'intégration de l'IA dans l'administration publique 2021-2026;
- Politique sur la sécurité de l'information du CSSL (RI-07-01-001);
- Politique relative à l'utilisation des services informatiques du CSSL (RI-07-05-005);
- Politique de confidentialité;
- Directive relative aux règles encadrant la gouvernance du CSSL à l'égard des renseignements personnels (DG-01-20-005).

5. Définitions

5.1 Intelligence artificielle (IA) :

Système automatisé qui, pour des objectifs explicites ou implicites, déduit, à partir d'entrées reçues, comment générer des résultats en sortie tels que des prévisions, des contenus, des recommandations ou des décisions qui peuvent influer sur des environnements physiques ou virtuels. Différents systèmes d'IA présentent des degrés variables d'autonomie et d'adaptabilité après déploiement.

5.2 Intelligence artificielle générative (IAG) :

Ensemble des techniques d'intelligence artificielle utilisées pour produire du contenu au moyen d'algorithmes et de mégadonnées, généralement sous forme de fichier texte, son, vidéo ou image.

5.3 Cas d'usage :

Description des exigences comportementales d'un système et de son interaction avec un utilisateur. Un cas d'usage décrit l'objectif des utilisateurs ainsi que les exigences, y compris la séquence d'interactions entre les utilisateurs et le système.

5.4 Renseignements personnels (RP) :

Toute information concernant une personne physique et permettant de l'identifier directement ou indirectement (ex. : nom, adresse, courriel personnel, date de naissance, dossier scolaire, informations médicales).

5.5 Données numériques gouvernementales (DNG) :

Actifs informationnels stratégiques régis par le MCN et la LGGRI (mobilité, qualité, sécurité, sources officielles).

5.6 Évaluation des facteurs relatifs à la vie privée (EFVP) :

Analyse obligatoire dans les situations prévues par la LAI (exemple : acquisition/développement d'un système impliquant des renseignements personnels).

5.7 Incident de confidentialité :

Accès, utilisation ou communication non autorisé d'un renseignement personnel, perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

6. Principes directeurs

L'utilisation de l'IA au CSSL repose sur les principes suivants (inspiré des principes exposés dans l'*Énoncé de principes pour une utilisation responsable de l'intelligence artificielle par les organismes publics* (MCN)) :

6.1 Intégrité et éthique

Toute utilisation de l'IA doit respecter des standards éthiques stricts. Avant de diffuser un contenu généré par l'IA, il est impératif de vérifier son exactitude et de s'assurer de l'absence de biais. De plus, l'origine de l'IA doit être divulguée, en précisant si le contenu est partiellement ou totalement généré par un outil d'IA.

6.2 Protection des renseignements personnels et confidentialité

L'entrée de renseignements personnels, confidentiels ou protégés (ex. : informations sur les élèves ou employés, documents internes sensibles) dans un outil d'IA, même approuvé, est **strictement interdite**.

6.3 Responsabilité et imputabilité

L'utilisateur demeure responsable du contenu généré par l'IA et doit s'assurer de sa validité, conformité et pertinence avant toute diffusion.

6.4 Utilisation encadrée

L'IA doit être utilisée dans un cadre pédagogique et administratif approuvé. Toute automatisation de prise de décision doit être validée par une instance humaine.

6.5 Sécurité et cybersécurité

L'usage des outils d'IA doit respecter les normes de cybersécurité établies par le CSSL et le gouvernement du Québec. Seuls les outils approuvés par le Service des technologies de l'information peuvent être utilisés.

7. Rôles et responsabilités

L'application efficace de la présente Politique repose sur la compréhension et le respect des rôles et responsabilités qui suivent :

7.1 Conseil d'administration

- Adopter la politique.

7.2 Direction générale

- Veiller à l'application de la politique et ajuster les balises au besoin pour garantir sa pertinence face à l'évolution rapide de l'IA.
- Allouer les ressources nécessaires (humaines, technologiques et financières), notamment pour la formation et la sécurisation des infrastructures.

7.3 Comité de gouvernance de l'IAG (CGIAG) (à mettre en place)

- Autoriser les cas d'usage des systèmes d'IAG en s'assurant d'un retour sur investissement, de l'obtention de bénéfices et d'une gestion des risques adéquate.
- Effectuer le suivi des risques, approuver les plans de mitigation, décider des arrêts et relances, notamment en cas de suspension gouvernementale.
- Élaborer et mettre en œuvre un programme de formation et de sensibilisation incluant minimalement les formations proposées par le MCN (risques liés à l'utilisation de l'IAG, usage responsable, etc.).
- Rendre disponible un guide interne prévoyant les cas d'usage autorisés et ceux qui sont interdits ou soumis à des restrictions.
- Tenir à jour le Registre des systèmes d'IAG et des cas d'usage prévu au paragraphe 8.2 de la Politique.
- Suivre les développements technologiques et proposer des orientations stratégiques à la direction générale.

7.4 Comité sur l'accès à l'information et la protection des renseignements personnels

- Veiller à l'application de la LAI (règles de gouvernance, EFVP, incidents de confidentialité, consentements) et à la tenue des registres requis.
- Analyser, prioriser et soumettre des recommandations sur les cas d'usage au comité de gouvernance de l'IAG (selon les composantes et les ressources disponibles).

7.5 Chef de la sécurité de l'information organisationnelle (CSIO)

- Appliquer la LGGRI et les indications d'application du MCN (contrôles techniques, classification, journalisation, restrictions d'outils).

7.6 Service des technologies de l'information (STI)

- Évaluer les systèmes d'IAG, notamment quant aux normes de sécurité, selon les recommandations du MCN.
- Mettre en place des mesures de cybersécurité pour protéger l'infrastructure contre les menaces spécifiques à l'IAG.
- Soutenir le personnel dans l'intégration technique des outils d'IAG approuvés et en assurer la maintenance de nos systèmes internes, le cas échéant.

7.7 Gestionnaires

- Mettre en œuvre la Politique et voir à son application uniforme dans tous les établissements et services.
- Promouvoir une culture de citoyenneté numérique responsable et d'intégrité intellectuelle auprès du personnel et des élèves.

7.8 Personnel enseignant

- Intégrer l'IAG de manière pédagogiquement pertinente et critique dans les activités, conformément aux objectifs d'apprentissage.
- Définir clairement aux élèves les consignes d'utilisation de l'IAG dans le cadre des travaux et évaluations.
- Modéliser l'utilisation éthique et responsable de l'IAG et développer la pensée critique des élèves face aux contenus générés.
- Protéger les renseignements personnels et les données institutionnelles en s'abstenant de les insérer dans les outils d'IAG.

7.9 Utilisateurs (membres du personnel, élèves, parents et tout autre utilisateur)

- Respecter la présente Politique.
- Utiliser uniquement les systèmes autorisés par le CSSL.
- Ne pas divulguer d'information confidentielle dans des systèmes non autorisés et signaler tout incident de confidentialité, le cas échéant.

7.10 Partenaires externes et fournisseurs

- Garantir la conformité légale de leurs solutions d'IAG lorsqu'elles sont utilisées par le CSSL.
- Fournir une transparence totale sur la manière dont les données du CSSL sont traitées, utilisées et sécurisées par leurs systèmes d'IAG.
- Respecter les ententes contractuelles et les exigences de sécurité du CSSL.

8. Processus d'évaluation d'un système d'IAG

Les cas d'usage des systèmes d'IAG sont pertinents si l'utilisation d'un tel système est essentielle à la résolution d'un problème réel, à l'amélioration d'un processus, à l'amélioration des services offerts à la population (efficience, efficacité et pertinence) ou à d'autres bénéfices (impacts positifs, gains, réduction des coûts).

Chacun des cas d'usage doit être documenté, en précisant notamment :

- La description générale du système d'IAG qui sera utilisé;
- La description générale de l'utilisation prévue du système d'IAG;

- La justification de la pertinence de l'utilisation prévue d'un système d'IAG;
- Une évaluation des gains anticipés.

Les cas d'usage doivent être analysés et priorisés en considérant non seulement les bénéfices anticipés, mais également les risques encourus.

8.1 Gestion des risques

Toute utilisation d'un système d'IAG doit être basée sur une démarche de gestion des risques. Cette démarche doit être exhaustive; elle doit notamment comprendre les étapes qui suivent :

- Identifier tous les risques organisationnels encourus par l'utilisation d'un système d'IAG. Ces risques peuvent, sans s'y limiter, être observés dans les matières suivantes : éthique, sécurité de l'information, gouvernance de données, juridique;
- Analyser les risques et documenter leurs principales causes et conséquences;
- Évaluer les risques et, en fonction notamment des résultats, prioriser leur traitement;
- Déterminer des mesures de mitigation, les responsables de leur mise en œuvre ainsi que les échéances;
- Approuver les résultats;
- Effectuer le suivi et la revue des risques en fonction du processus organisationnel défini.

Dès la phase de conception d'un projet d'acquisition, de développement ou de refonte d'un système d'IAG, et lors de la définition des cas d'usage, le CSSL doit procéder à une ÉFVP. Cette ÉFVP doit être actualisée tout au long des phases d'expérimentation, de développement et de déploiement du projet qui concerne un système d'IAG. Le cas échéant, la direction générale doit accepter le niveau de risque résiduel d'atteinte à la vie privée pour poursuivre les activités. Cette exigence vaut pour tous les systèmes d'IAG incluant ceux qui, à première vue, ne semblent pas impliquer de renseignements personnels. Dans le cas de ces derniers, le CSSL doit procéder à l'ÉFVP laquelle pourra confirmer l'absence de renseignements personnels.

La démarche de gestion des risques, incluant l'ÉFVP, doit être révisée périodiquement en fonction de l'évolution du système d'IAG et de son contexte d'utilisation.

8.2 **Registre des systèmes d'IAG et des cas d'usage** (à venir selon si des ressources et des fonctionnalités sont disponibles à cet effet)

Le CSSL tient un registre des systèmes d'IAG et des cas d'usage recensant les finalités, les données utilisées et leurs catégories (incluant présence de renseignements personnels), emplacements et accès, fournisseurs, mesures de sécurité, EFVP, décisions prises, responsables, périodes de révision et toute autre information pertinente.

8.3 Mesures liées au cycle de vie d'un système d'IAG

8.3.1 Planification et conception

- Évaluer les risques pour démontrer l'intérêt public, l'alignement stratégique et l'absence de solutions moins intrusives.

8.3.2 Collecte et traitement des données

- Déterminer si des renseignements personnels sont en jeu, déclencher l'EFVP et consulter le Comité sur l'accès à l'information et la protection des renseignements personnels.
- Promouvoir la qualité et la conformité des données numériques utilisées dans un système d'IAG tout au long de leur cycle de vie (création, collecte, conservation, utilisation, transmission, communication, archivage et destruction).
- Appliquer le Modèle de classification de sécurité des données numériques gouvernementales approuvé par le MCN pour protéger les DNG utilisées.

- Interdire toute saisie de renseignements de nature confidentielle dans un système d'IAG.

8.3.3 Construction du modèle ou adaptation d'un modèle existant

- Privilégier des environnements gouvernementaux ou contractualisés (infonuagique conforme).
- Favoriser un contrôle strict des droits d'accès au système d'IAG.
- Respecter les consignes en vigueur, notamment quant aux suspensions ou limitations.
- Dans tout contrat avec un fournisseur, intégrer des clauses portant sur : résidence/lieu de traitement, usage secondaire, conservation/suppression, traçabilité, droits d'audit, gestion d'incidents, biais et performance.

8.3.4 Test, évaluation, vérification et validation des systèmes internes d'IAG

- Mettre en place des tests de performance (efficience et qualité des résultats) pour vérifier la fiabilité et la robustesse du système d'IAG et apporter les ajustements requis avant le déploiement.
- Établir un processus d'amélioration continue pour chaque système d'IAG utilisé, le documenter et l'appliquer. Ce processus vise à s'assurer que le système d'IAG demeure efficace et conforme à une utilisation responsable.
- Développer un plan de supervision humaine adéquate et une journalisation des interactions.
- Prendre les moyens afin que tout système d'IAG utilisé ayant un impact sur des décisions, des prédictions ou des actions concernant les citoyens ou les entreprises, intègre des mécanismes qui assurent des explications claires et sans ambiguïté. L'utilisation de modèles d'IAG ouverts[1], lorsque cela est possible, doit alors être privilégiée.

8.3.5 Mise à disposition pour utilisation

- Élaborer et mettre en œuvre un programme de formation et de sensibilisation aux risques liés à l'utilisation du système d'IAG, incluant une mise à jour des connaissances lorsque nécessaire.
- Promouvoir une gestion du changement adaptée à l'impact organisationnel de l'introduction d'un système d'IAG et permettre l'introduction de cette technologie de manière optimale.

8.3.6 Exploitation et suivi

- Effectuer une surveillance continue du système d'IAG, notamment par des mesures pour vérifier sa fiabilité, sa robustesse et son utilisation responsable.
- Faire une mise à jour des mesures de sécurité applicables.
- Effectuer une revue périodique des modèles, des jeux de données, des dérives, des biais et des incidents.
- Établir une convention d'usage.

8.3.7 Mise hors service

- Procéder à un arrêt de service si non-conformité, en cohérence avec les indications du MCN.
- Supprimer ou désactiver les accès au système d'IAG.
- Effectuer, en vertu d'une obligation de moyen, la gestion des données du système d'IAG, notamment par leur archivage ou leur destruction conformément au calendrier de conservation du CSSL.

[1] Un modèle d'IAG ouvert est un modèle dont au moins certains des composants (code, paramètres finaux, documentation, etc.) sont rendus publiquement accessibles, et ce, dans un cadre de licences et d'informations qui permettent son usage, son étude, sa modification ou sa redistribution. Le degré d'ouverture peut varier.

9. Encadrement de l'utilisation de l'intelligence artificielle

9.1 Usages autorisés

L'IA peut être utilisée, sous supervision et validation humaine, pour les activités suivantes :

- Rédaction et correction de documents administratifs et pédagogiques.
- Analyse et synthèse de données dans un cadre décisionnel (sans informations confidentielles).
- Soutien à l'apprentissage pour la création de contenus pédagogiques et la personnalisation de l'enseignement.
- Optimisation des tâches administratives, notamment pour la planification et la gestion des ressources.

9.2 Usages interdits

L'IA ne doit en aucun cas être utilisée pour :

- Saisir ou traiter des renseignements personnels ou sensibles.
- Produire des décisions automatisées sans validation humaine.
- Générer du contenu trompeur, biaisé, discriminatoire, diffamatoire ou contraire aux valeurs éducatives.
- Ne pas respecter la *Loi sur les droits d'auteur* ou la propriété intellectuelle.
- Utiliser des outils d'IA non approuvés par le CSSL.

10. Outils autorisés et recommandations

10.1 Outils d'intelligence artificielle approuvés

Le CSSL valide certains outils d'IA pour une utilisation professionnelle et éducative.

- Pour les employés, seules les plateformes autorisées par le Service des technologies de l'information peuvent être utilisées (ex. : Microsoft Copilot, ChatGPT (OpenAI), Google Gemini).
- Pour les élèves, l'usage de l'IA est limité aux plateformes validées par le Service des ressources éducatives, les enseignants et la direction.

10.2 Précautions à prendre avant d'utiliser un outil d'intelligence artificielle

Avant d'utiliser un outil d'IA, l'utilisateur doit se poser les questions suivantes :

- Cet outil est-il approuvé par le CSSL?
- Ai-je validé l'exactitude et la fiabilité du contenu généré?
- Mon usage de l'IA respecte-t-il la confidentialité des données?
- L'IA remplace-t-elle un travail critique nécessitant un jugement humain?

11. Sanctions en cas de non-respect

Toute utilisation non conforme à cette politique peut entraîner des mesures disciplinaires, allant d'un avertissement à une suspension des accès ou d'autres sanctions selon la gravité du manquement.

12. Entrée en vigueur et mise à jour

Cette politique entre en vigueur dès son adoption par le CSSL et sera révisée périodiquement afin d'être adaptée aux évolutions technologiques et légales.