

POLITIQUE RELATIVE À LA GOUVERNANCE DE L'INTELLIGENCE ARTIFICIELLE GÉNÉRATIVE

SERVICE DISPENSATEUR :

Service du secrétariat général et des
communications

PREMIÈRE ADOPTION :
(n° de résolution)

Le 30 juin 2026 (CA-0761-06-26)

MODIFICATIONS :
(n°s de résolutions)

1. BUT ET 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 déclassé des systèmes d'intelligence artificielle générative (IAG) au sein du Centre de services scolaire du Pays-des-Bleuets (CSSPB), en conformité avec les exigences légales et gouvernementales applicables, ainsi que dans le respect des conventions collectives en vigueur. Elle vise à :

- Assurer un usage responsable, transparent et sécuritaire de l'IAG dans l'administration publique;
- Protéger les renseignements personnels et les données numériques gouvernementales;
- Garantir la conformité aux lois, politiques et indications d'application gouvernementales;
- Favoriser des bénéfices mesurables pour la population, en soutenant les services publics et la reddition de comptes.

2. CHAMP D'APPLICATION

La Politique s'applique :

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

3. ENCADREMENT LÉGAL

La Politique prend assise notamment sur les encadrements suivants :

- [Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement](#) (LGRI);
- [Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels](#) (LAI);
- 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);

- Secrétariat du Conseil du trésor (SCT) – [Stratégie d'intégration de l'intelligence artificielle dans l'administration publique 2021-2026](#) (SCT);
- Les conventions collectives, le *Règlement déterminant certaines conditions de travail des cadres des commissions scolaires* et du Comité de gestion de la taxe scolaire de l'Île de Montréal.

4. DÉFINITIONS

- 4.1 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 influencer sur des environnements physiques ou virtuels. Différents systèmes d'IA présentent des degrés variables d'autonomie et d'adaptabilité après déploiement.
- 4.2 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.
- 4.3 Système d'IAG public :** toute version accessible au grand public de systèmes d'IAG, qu'elle soit gratuite ou payante, notamment celles offertes en ligne.
- 4.4 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.
- 4.5 Renseignements personnels (RP) :** renseignements qui concernent une personne physique et permettent, directement ou indirectement, de l'identifier (ex. : nom, adresse, courriel personnel, date de naissance, dossier scolaire, informations médicales, photographies).
- 4.6 Données numériques gouvernementales (DNG) :** actifs informationnels stratégiques régis par le MCN et la LGGRI (mobilité, qualité, sécurité, sources officielles).
- 4.7 Évaluation des facteurs relatifs à la vie privée (EFVP) :** démarche évolutive visant à protéger les renseignements personnels et à assurer le respect de la vie privée tout au long d'un projet, notamment l'acquisition et le développement d'un système impliquant des renseignements personnels. Elle permet d'évaluer la conformité aux lois applicables, d'identifier les risques d'atteinte à la vie privée et de mettre en place des mesures pour les prévenir ou les atténuer.
- 4.8 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.

5. PRINCIPES

La présente Politique repose sur des principes inspirés de l'*Énoncé de principes pour une utilisation responsable de l'intelligence artificielle par les organismes publics* du gouvernement du Québec. Ces principes doivent guider l'ensemble des activités, décisions et pratiques liées à leur utilisation au sein de l'organisation, à savoir :

- 5.1** L'utilisation des technologies numériques et de l'intelligence artificielle doit respecter les droits et libertés, la dignité humaine, la vie privée ainsi que les lois applicables. Les renseignements personnels et informations confidentielles doivent être protégés par des mesures de sécurité adaptées.
- 5.2** Le CSSPB favorise une utilisation transparente et éthique de l'intelligence artificielle, en limitant les biais et la discrimination et en permettant une compréhension raisonnable de leur utilisation.
- 5.3** L'utilisation des technologies demeure sous la responsabilité de l'organisation et de son personnel. Les rôles et responsabilités doivent être clairement définis et le jugement humain maintenu dans les décisions importantes.
- 5.4** Les systèmes utilisés doivent être fiables, sécuritaires et adaptés aux besoins. Des mécanismes de contrôle, de validation, de suivi et d'amélioration continue doivent être appliqués de manière proportionnelle aux risques et aux impacts potentiels.
- 5.5** Le CSSPB soutient le développement des connaissances et des compétences nécessaires à une utilisation responsable des technologies et révisé périodiquement ses pratiques afin de suivre l'évolution des technologies, des risques et des obligations légales.

6. RÔLES ET RESPONSABILITÉS

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

6.1. Centre de services scolaire

- Adopter la présente Politique et en assurer la revue périodique pour garantir sa pertinence face à l'évolution rapide de l'IA.
- Allouer, dans la mesure du possible, les ressources nécessaires (humaines, technologiques et financières), notamment pour la formation et la sécurisation des infrastructures.

6.2. Comité de sécurité informatique

- 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.
- 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 8.3 de la Politique en collaboration avec le comité IA du CSSPB.
- Suivre les développements technologiques et proposer des orientations stratégiques à la direction générale.

6.3. Le comité IA du CSSPB

- Élaborer et mettre en œuvre un programme de formation continue et de sensibilisation aux risques liés à l'utilisation de systèmes d'IAG afin de veiller à ce que les membres du personnel disposent des compétences pour utiliser ces systèmes de manière responsable, incluant minimalement les formations proposées par le MCN (risques liés à l'utilisation de l'IAG, usage responsable, etc.).
- Collaborer avec le comité de sécurité informatique et le comité pédagognumérique du CSSPB afin de diffuser dans les milieux scolaires les systèmes et outils d'IAG autorisés par le CSSPB.

6.4. Responsable de l'accès à l'information et de 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, accompagné du comité de l'accès à l'information et de la protection des renseignements personnels (CAIPRP).
- Évaluer le niveau de risque résiduel d'atteinte à la vie privée d'un système d'IAG.
- Analyser, prioriser et soumettre des recommandations sur les cas d'usage au comité de sécurité informatique.

6.5. 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).

6.6. Service des ressources informatiques (SRI)

- Évaluer les systèmes d'IAG, notamment quant aux normes de sécurité.
- 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.

6.7. Gestionnaires

- Mettre en œuvre la Politique et veiller 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.

6.8. Personnel enseignant

- Respecter la présente Politique et toute autre décision du CSSPB à l'égard de l'utilisation de l'IAG dans le cadre de ses fonctions.
- Utiliser uniquement les systèmes autorisés par le CSSPB.
- Intégrer l'IAG en classe dans un cadre strictement pédagogique en assurant une supervision adéquate, conformément aux objectifs d'apprentissage.
- Définir clairement aux élèves les consignes d'utilisation de l'IAG dans le cadre des travaux et évaluations, sous réserve de respecter l'âge minimal d'utilisation de l'application et de l'obtention des consentements nécessaires au préalable (titulaires de l'autorité parentale, directions d'établissement, etc.), s'il a lieu.
- 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.

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

- Respecter la présente Politique et toute autre décision du CSSPB à l'égard de l'utilisation de l'IAG dans le cadre de leurs fonctions.
- Utiliser uniquement les systèmes autorisés par le CSSPB.
- Ne pas divulguer d'information confidentielle dans des systèmes publics et signaler tout incident de confidentialité, le cas échéant.
- Protéger les renseignements personnels et les données institutionnelles en s'abstenant de les insérer dans les outils d'IAG.

6.10. Partenaires externes et fournisseurs

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

7. UTILISATION DES SYSTÈMES D'IAG PUBLICS

L'utilisation des systèmes d'IAG publics est plus amplement balisée dans la Directive visant à baliser l'utilisation de l'intelligence artificielle générative du CSSPB. Cette Directive précise les responsabilités du personnel et les conditions d'utilisation pour les élèves, tout en soutenant la mission éducative et l'intégration progressive de ces outils.

8. PROCESSUS D'ÉVALUATION D'UN SYSTÈME D'IAG

Les prochaines étapes visent davantage le développement et l'acquisition, par le CSSPB, d'outils d'intelligence artificielle générative (IAG) intégrés aux processus internes de l'organisation. Cette démarche permettra d'assurer une utilisation cohérente et efficiente de ces technologies, en lien avec les orientations organisationnelles. Leur mise en œuvre reposera sur la contribution des différents acteurs et comités, conformément aux rôles définis à la section 6 de la Politique.

8.1. Priorisation des cas d'usage

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. Au surplus, il y a lieu de prioriser l'utilisation de systèmes d'IAG privés sécurisés.

8.2. 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 être observés dans les matières suivantes, entre autres : 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'IAI, et lors de la définition des cas d'usage, le CSSPB doit procéder à une EFVP. Cette EFVP doit être actualisée tout au long des phases d'expérimentation, de développement et de déploiement du projet qui concerne un système d'IAI. Le cas échéant, le CAIPRP 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'IAI incluant ceux qui, à première vue, ne semblent pas impliquer de renseignements personnels. Dans le cas de ces derniers, le CSSPB doit procéder à l'EFVP laquelle pourra confirmer l'absence de renseignements personnels.

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

8.3. Registre des systèmes d'IAI et des cas d'usage

Le CSSPB tient un registre des systèmes d'IAI 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.

8.4. Mesures liées au cycle de vie d'un système d'IAI

8.4.1. Planification et conception

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

8.4.2. Collecte et traitement des données

- Déterminer si des renseignements personnels sont impliqués, effectuer l'EFVP et consulter le CAIPRP.
- Assurer la qualité et la conformité des données numériques utilisées dans un système d'IAI 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 public.

8.4.3. Construction du modèle ou adaptation d'un modèle existant

- Privilégier des environnements gouvernementaux ou contractualisés (infonuagiques conformes).
- Assurer 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.

8.4.4. Test, évaluation, vérification et validation

- Mettre en place des tests de performance (efficacité 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.
- S'assurer 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 ouverts¹, lorsque cela est possible, doit alors être privilégiée.

8.4.5. 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.
- Assurer 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.

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.

8.4.6. Exploitation et suivi

- Assurer une surveillance continue du système d'IAG, notamment par des mesures pour vérifier sa fiabilité, sa robustesse et son utilisation responsable.
- S'assurer de la 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.

8.4.7. Mise hors service

- Procéder à un arrêt de service en cas de non-conformité, en cohérence avec les indications du MCN.
- Supprimer ou désactiver les accès au système d'IAG.
- Assurer la gestion des données du système d'IAG, notamment par leur archivage ou leur destruction conformément au calendrier de conservation du CSSPB.

9. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur le jour suivant son adoption par le conseil d'administration.