Centre de services scolaire des Grandes-Seigneuries
Québec

PROCÉDURE

RELATIVE À L'UTILISATION DE L'INTELLIGENCE ARTIFICIELLE GÉNÉRATIVE (IAG)

 # 30-02

Adoption le : 2 juin 2026
Mise en vigueur le : 3 juin 2026
Décision : BDG-20260602-887

Autorisation :

Christian Duval
Directeur général

1. Contexte et objectif

L'intelligence artificielle générative (IAG) transforme de façon significative les pratiques professionnelles et pédagogiques. Son utilisation doit s'effectuer de manière responsable, éthique et conforme au cadre légal en vigueur, tout en assurant la protection des renseignements de l'organisation.

La présente procédure a pour objectif d'encadrer l'utilisation de l'IAG. Elle vise notamment à :

- Établir une structure de gouvernance visant une utilisation responsable de l'IAG.
- Encadrer l'intégration de l'IAG dans les activités professionnelles et pédagogiques.
- Promouvoir une utilisation transparente, éclairée et sécuritaire de l'IAG.
- Sensibiliser le personnel aux enjeux éthiques, juridiques et pédagogiques liés à l'IAG.
- Prévenir les risques associés à la confidentialité, aux biais et à la propriété intellectuelle.
- Protéger les renseignements personnels et les données numériques gouvernementales.
- Soutenir le développement de compétences numériques responsables.

La présente procédure s'inscrit dans le cadre de la *politique relative à la sécurité de l'information, à l'utilisation des ressources informationnelles et à la protection des renseignements personnels* du CSSDGS.

2. Encadrement

- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1).
- *Loi sur le droit d'auteur* (L.R.C., 1985, c. C42).
- *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics* (RLRQ, c. G-1.03).
- *Énoncé de principes pour une utilisation responsable de l'intelligence artificielle par les organismes publics* (arrêté numéro 2025-02 du ministre de la Cybersécurité et du Numérique en date du 3 décembre 2025).
- *Mesures applicables lors de l'utilisation de l'intelligence artificielle générative Indication d'application* (indication d'application IA-RI-2025-003-OP du ministère de la Cybersécurité et du Numérique en date du 5 décembre 2025).
- *Stratégie d'intégration de l'intelligence artificielle dans l'administration publique 2021-2026* du Secrétariat du Conseil du trésor.

3. Définitions

3.1 Données numériques gouvernementales (DNG)

Toute information portée par un support technologique, incluant un support numérique, détenue par un organisme public, sous réserve des exclusions prévues à l'alinéa 2 de l'article 12.10 de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*.

3.2 Évaluation des facteurs relatifs à la vie privée (EFVP)

Analyse d'impact visant à protéger les renseignements personnels et à respecter la vie privée des personnes physiques. Elle consiste à considérer, avant de commencer un projet et tout au long de sa durée, tous les facteurs (conformité à la législation et aux principes, analyse des risques, stratégies d'atténuation) ayant un effet positif ou négatif sur la vie privée des personnes concernées.

3.3 Incident de confidentialité

L'accès, l'utilisation et la communication non autorisés par la loi d'un renseignement personnel, ainsi que la perte de ce renseignement ou toute autre atteinte à sa protection.

3.4 Intelligence artificielle

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.

3.5 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.

3.6 Renseignement personnel (RP)

Renseignement qui concerne une personne physique et permet directement ou indirectement de l'identifier.

3.7 Système d'intelligence artificielle générative ouvert

Système d'intelligence artificielle générative dont le fonctionnement repose sur un modèle accessible, transparent et documenté, permettant de comprendre, d'expliquer

et, dans certains cas, de reproduire les mécanismes ayant mené aux résultats générés.

3.8 Système d'intelligence artificielle générative privé sécurisé

Système d'IAG utilisé dans un environnement contrôlé et non accessible au grand public, généralement en circuit fermé, dont l'hébergement, les données, les accès et l'utilisation sont soumis à des mesures de sécurité, de gouvernance et de protection des renseignements conformes aux exigences du CSSDGS.

3.9 Système d'intelligence artificielle générative public

Toute version « grand public » gratuite ou non de systèmes d'IAG, comme les versions en ligne de Copilot (incluant Copilot Chat) et ChatGPT, accessible par le web à l'extérieur du CSSDGS.

3.10 Système d'intelligence artificielle générative spécialisé (ou vertical)

Système d'IAG spécifique à un secteur d'activité, un domaine professionnel ou un contexte organisationnel précis et soumis à un cadre normatif propre à ce champ d'application.

3.11 Utilisateur

Toute personne qui fait usage d'un système d'IAG.

4. Champ d'application

La procédure s'applique :

a) à toutes les personnes en lien avec le CSSDGS :
- Les membres du personnel;
- Les élèves inscrits dans les établissements du CSSDGS et leurs parents;
- Les consultants, stagiaires et tout tiers travaillant pour ou avec le CSSDGS et ayant accès aux environnements numériques ou aux données de l'organisation;
- Les partenaires externes, fournisseurs et prestataires de services.

b) à tout système d'IAG (interne, infonuagique, tiers, codage interface de programmation d'application (API), connecteurs) utilisé dans le cadre des fonctions du CSSDGS;

c) à toutes les données détenues par le CSSDGS et aux DNG.

5. Principes directeurs

5.1 Principes directeurs

Les principes qui suivent sont ceux énoncés dans l'*Énoncé de principes pour une utilisation responsable de l'intelligence artificielle par les organismes publics* du ministre de la Cybersécurité et du Numérique en date du 3 décembre 2025. Lorsqu'applicables, ils ont été bonifiés des principes énoncés dans la *Politique relative à la sécurité de l'information, à l'utilisation des ressources informationnelles et à la protection des renseignements personnels* du CSSDGS.

5.1.1 Respect des personnes et de la règle de droit

L'IAG doit être utilisée dans le respect des lois, des droits fondamentaux et de la vie privée.

Les utilisations de l'IAG doivent également respecter les droits de propriété intellectuelle, dont les droits d'auteur, les licences, les brevets et le droit des marques de commerce.

5.1.2 Inclusion, équité et éthique

L'IAG doit permettre de servir toute la population, sans exclure certains groupes et sans accentuer les inégalités. Les contenus doivent promouvoir l'équité, l'inclusion et la diversité des perspectives.

Le recours à l'IAG doit se faire de manière éthique en prenant en considération les risques de biais et mettant en place des mesures afin de les identifier et de les corriger.

5.1.3 Fiabilité, robustesse et évolution

Les systèmes d'IAG doivent fonctionner correctement et de façon stable et constante. Les données utilisées lors de requêtes faites à un système d'IAG doivent être de bonne qualité et sans biais importants.

Des tests et des contrôles doivent être faits régulièrement afin de tenir compte des changements juridiques, organisationnels, technologiques, physiques ou environnementaux ainsi que de l'évolution des menaces et des risques.

5.1.4 Sécurité de l'information et protection des renseignements personnels

L'utilisation des systèmes d'IAG doit respecter les obligations relatives à la sécurité de l'information. Afin de limiter les risques, des mesures de sécurité doivent être mises en place pour protéger l'information, les renseignements personnels et les données confidentielles.

5.1.5 Efficience, efficacité et pertinence

L'IAG ne doit être utilisée que lorsqu'elle apporte une valeur ajoutée adaptée aux besoins réels du CSSDGS et que les risques identifiés peuvent être gérés de manière proportionnée. L'utilisateur doit pouvoir expliquer et justifier l'usage de l'IAG dans tout document ou projet produit.

5.1.6 Durabilité
L'utilisation de l'IAG doit se faire dans une optique de sobriété numérique, en limitant l'impact environnemental et la surutilisation des outils. Elle doit prendre en considération que la génération d'images, de vidéos et d'audio entraine une empreinte écologique plus importante que la génération de texte.

5.1.7 Transparence
L'utilisation de l'IAG gagne à être divulguée de manière claire, traçable et proportionnée. Le modèle de divulgation suivant peut être utilisé :

« L'intelligence artificielle générative a été utilisée pour [motif, ex. : l'idéation/la reformulation/la synthèse]. Le contenu a été vérifié et validé.»

Dans un contexte pédagogique, tout contenu généré par l'IAG présenté ou remis à des élèves, parents, collègues ou partenaires, gagne à être explicitement mentionné.

5.1.8 Explicabilité
Lorsqu'une décision, une prédiction ou une action utilise l'IAG, le CSSDGS doit être en mesure d'expliquer aux personnes concernées comment celle-ci a été effectuée. Lorsqu'il est possible et pertinent de le faire, le CSSDGS doit utiliser un système d'IAG ouvert permettant de faciliter la compréhension, la reproductibilité et l'explicabilité des résultats.

5.1.9 Responsabilité et imputabilité
Le CSSDGS est entièrement responsable de toute utilisation de l'IAG et doit mettre en place une structure de gouvernance promouvant l'utilisation responsable de l'IAG.

Il est de la responsabilité de l'utilisateur de l'IAG de vérifier l'exactitude, de détecter et corriger les biais, de citer les sources consultées et de documenter la démarche, le cas échéant.

5.1.10 Compétence
Le CSSDGS doit former son personnel à l'utilisation de l'IAG et à ses enjeux.

5.1.11 Autonomie et supervision humaine
L'utilisation de l'IAG afin d'appuyer ou de prendre une décision automatisée doit préalablement être approuvée par le Comité sur la protection des renseignements personnels et la sécurité de l'information (CPRPSI) du CSSDGS afin d'assurer la conformité aux modalités prévues à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.*

Par ailleurs, avant de recourir à l'IAG dans le cadre d'un processus décisionnel, le consentement de la personne concernée doit être obtenu.

En tout temps, il doit être possible pour un humain d'intervenir, de valider ou d'arrêter l'IAG.

5.1.12 Souveraineté numérique

Le CSSDGS doit tendre à réduire sa dépendance aux fournisseurs étrangers. Lorsque possible, il doit privilégier des fournisseurs québécois ou canadiens offrant des solutions hébergées au Québec.

6. Systèmes d'IAG

6.1 Systèmes d'IAG approuvés

Le CSSDGS tient à jour un inventaire des systèmes d'IAG publics et privés sécurisés approuvés sur Maestro.

Pour chaque système approuvé, les types d'usages permis, restreint ou interdit sont répertoriés.

Toute utilisation non conforme aux types d'usages autorisés est strictement interdite.

6.2 Règles d'utilisation

Il revient à l'utilisateur d'effectuer les vérifications requises afin de s'assurer que son utilisation est conforme aux exigences de l'organisation, notamment en matière de sécurité de l'information et de protection des renseignements personnels. S'il n'est pas en mesure de réaliser ces vérifications lui-même ou si un doute subsiste, il doit en informer son supérieur immédiat et s'abstenir d'utiliser le système.

Notamment, il est interdit d'entrer des renseignements personnels ou des données confidentielles dans des systèmes d'IAG publics. Les usages impliquant de tels renseignements ou données ne peuvent se réaliser que dans des systèmes d'IAG privés sécurisés.

6.3 Processus d'approbation d'un système d'IAG

6.3.1 Demande

Le demandeur doit remplir une demande selon les modalités prévues à l'Annexe 1.

Il revient au demandeur de requérir la collaboration des personnes pertinentes afin de fournir les informations attendues dans le cadre de la demande.

6.3.2 EFVP

La réalisation d'une EFVP est obligatoire pour tout système d'IAG faisant l'objet d'une demande d'approbation, même lorsque le système d'IAG ne semble pas, à première vue, impliquer de renseignements personnels.

Le demandeur doit s'assurer de la réalisation d'une EFVP en suivant la procédure du

CSSDGS relative aux EFVP.

L'EFVP doit être réalisée dès la phase de conception d'un projet d'acquisition, de développement ou de refonte d'un système d'IAG et être actualisée tout au long des phases d'expérimentation, de développement et de déploiement du projet qui concerne un système d'IAG. Elle doit également être révisée périodiquement en fonction de l'évolution du système d'IAG et de son contexte d'utilisation.

6.3.3 Analyse des demandes

Toute demande relative à l'approbation d'un système d'IAG doit être soumise au Comité de direction en intelligence numérique (CODIR-IN) pour approbation.

Le CODIR-IN doit analyser et statuer sur les demandes en fonction, notamment, des éléments suivants :

- Le respect des principes et des modalités prévus à la présente procédure;
- L'utilisation d'un système d'IAG privé sécurisé plutôt qu'un système d'IAG public;
- L'utilisation d'un système d'IAG spécialisé (ou vertical), lorsqu'il est disponible et économiquement viable;
- La priorisation des cas d'usage des systèmes d'IAG en fonction du retour sur investissement, de l'obtention des bénéfices et d'une gestion de risques adéquate;
- L'utilisation d'un modèle d'IAG ouvert lorsque le contexte nécessite une traçabilité complète et une reproductibilité des résultats, notamment lorsqu'il touche des services aux citoyens;
- L'utilisation d'un système d'IAG ouvert lors d'impact sur des décisions, des prédictions ou des actions concernant les citoyens ou les entreprises, afin d'être en mesure de fournir des explications claires et sans ambiguïté;
- Le recours à des fournisseurs québécois ou canadiens offrant des solutions hébergées au Québec ou au Canada lorsque les DNG comprennent des renseignements confidentiels.

7. Formation

Le Comité de direction en intelligence numérique (CODIR-IN) est responsable d'assurer la mise en œuvre d'un programme de formation et de sensibilisation **de base**, afin de garantir que l'ensemble du personnel possède les compétences nécessaires pour utiliser les systèmes d'IAG de manière responsable. Ce programme doit comporter les formations du ministère de la Cybersécurité et du Numérique, lorsqu'elles sont disponibles.

Toute demande relative à l'approbation d'un système d'IAG doit inclure un programme de formation **adaptée** et permettant d'assurer une gestion du changement spécifique à l'impact de ce système d'IAG sur le CSSDGS et ses utilisateurs.

8. Rôles et responsabilités

Direction générale
Approuve la présente procédure.

Alloue les ressources nécessaires (humaines, technologiques et financières), notamment pour la formation et la sécurisation des infrastructures.

Comité de direction en intelligence numérique (CODIR-IN)
Statue sur toute demande d'approbation relative à l'utilisation d'un système d'IAG et sur les cas d'usage permis, restreint et interdit.

Encadre et s'assure de la mise en œuvre d'un programme de formation et de sensibilisation de base.

Comité sur la protection des renseignements personnels et la gouvernance des données
Approuve l'utilisation de l'IAG destinée à appuyer ou à prendre une décision automatisée.

Exerce les rôles et responsabilités prévus à la Procédure concernant l'évaluation des facteurs relatifs à la vie privée (EFVP).

SGC
Est responsable de toute analyse éthique et légale en lien avec l'IAG.

Collabore à la mise à jour et application de la présente procédure.

SPOA
Collabore à la mise à jour et application de la présente procédure.

Élabore et promeus la gouvernance des données utilisées avec l'IAG.

STI
Est responsable de la mise à jour et de l'application de la présente procédure.

Soutien le personnel dans les pratiques pédagogiques numériques en lien avec les techniques d'enseignement et d'apprentissages utilisant l'IAG (compétence numérique et ses dimensions).

Établit et met à jour le moyen afin de faire une demande d'approbation d'un système d'IAG.

Soutien le demandeur pour toute demande relative à un nouveau système d'IAG.

Est responsable de toute analyse informatique et technique en lien avec l'IAG, notamment quant aux normes de sécurité.

Soutien le personnel dans l'intégration technique des systèmes d'IAG approuvés et en assure la gestion opérationnelle.

Suit les développements technologiques et propose des orientations stratégiques à la direction générale.

Cadre
Met en œuvre la procédure et veille à son application uniforme dans tous les établissements et services.

Promeut une culture de citoyenneté numérique responsable et d'intégrité intellectuelle auprès du personnel et des élèves.

Personnel enseignant
Intègre l'IAG de manière pédagogiquement pertinente et critique dans les activités, conformément aux objectifs d'apprentissage.

Communique clairement aux élèves les consignes d'utilisation de l'IAG dans le cadre des travaux et évaluations.

Modélise l'utilisation éthique et responsable de l'IAG et développe la pensée critique des élèves face aux contenus générés.

Protège les renseignements personnels et les données institutionnelles en s'abstenant de les insérer dans les systèmes d'IAG non approuvés.

Utilisateurs (membres du personnel, élèves, parents et tout autre utilisateur)
Respecte la présente procédure.

Utilise uniquement les systèmes autorisés par le CSSDGS.

Protège les renseignements personnels et les données institutionnelles en s'abstenant de les insérer dans les systèmes d'IAG non approuvés.

Signale tout incident de confidentialité, le cas échéant, au moyen du formulaire de déclaration disponible sur Maestro.

Partenaire externe, fournisseur et prestataire de service
Garantit la conformité légale de ses solutions d'IAG lorsqu'elles sont utilisées par le CSSDGS.

Fournit une transparence totale sur la manière dont les données du CSSDGS sont traitées, utilisées et sécurisées par ses systèmes d'IAG.

Respecte les ententes contractuelles, la présente procédure et les exigences de sécurité du CSSDGS.

9. Mécanisme de révision

La modification de la présente procédure se fait par la direction du Service des technologies de l'information et doit être autorisée par la direction générale.

10. Dispositions finales

La présente procédure entre en vigueur le 2 juin 2026.

Annexe 1
Demande d'approbation d'un système d'IAG

Toute demande d'approbation d'un système d'IAG doit s'effectuer par le moyen établi par le STI.

Le moyen établi par le STI doit, minimalement, permettre de recueillir les informations suivantes :

- **Informations à fournir par le demandeur**
  - Description générale du système d'IAG qui sera utilisé
  - Description générale de l'utilisation prévue du système d'IAG
  - Justification de la pertinence de l'utilisation prévue du système d'IAG
  - Évaluation des gains anticipés
  - Programme de formation comportant :
    - Sensibilisation aux risques liés à l'utilisation du système d'IAG;
    - Modalités d'utilisation responsable et sécuritaire du système d'IAG;
    - Calendrier de formation assurant que le personnel sera formé avant le déploiement du système d'IAG;
    - Modalités permettant d'assurer une veille afin de mettre à jour les connaissances, si requises.
  - Gestion du changement :
    - Modalités afin de prendre en considération la gestion du changement afin que l'introduction du système d'IAG soit optimale.

- **Informations à fournir par le demandeur appuyé par le STI**
  - Gestion des risques :
    - Risques organisationnels encourus par l'utilisation du système d'IAG;
    - Analyse des principales causes et conséquences des risques;
    - Évaluation des risques et priorisation de leur traitement en fonction, notamment des résultats;
    - Mesures de mitigation, responsables de leur mise en œuvre ainsi que les échéances;
    - Résultats de l'analyse de risques;
    - Modalités afin de faire le suivi et la revue des risques.
  - Impacts :
    - Mécanisme prévu pour évaluer les impacts, avant et après le déploiement du système d'IAG, d'afin d'assurer un suivi continu.
  - Supervision humaine :
    - Mécanisme prévu pour assurer une supervision humaine et pour évaluer l'impact potentiel des décisions et du degré d'autonomie du système d'IAG;
    - Mécanisme assurant des explications claires et sans ambiguïté lorsque l'IAG a un impact sur des décisions, des prédictions ou des actions concernant les citoyens.
  - Amélioration continue :
    - Processus d'amélioration continue pour le système d'IAG et modalités pour vérifier la fiabilité et la robustesse du système IAG.

- DNG :
  - DNG qui seront utilisées dans le système d'IAG, tout au long du cycle de vie de ces données (création, collecte, conservation, utilisation, transmission, communication, archivage et destruction);
  - Profil de mesures de sécurité attribué ou selon le cas, marquage des DNG utilisées pour chaque cas d'usage;
  - Classification et étiquetage des DNG en conformité avec le modèle de classification de sécurité des DNG;
  - Modalités de contrôle prévues au seuil minimal de sécurité;
  - Modalités de gestion stricte des accès aux DNG.