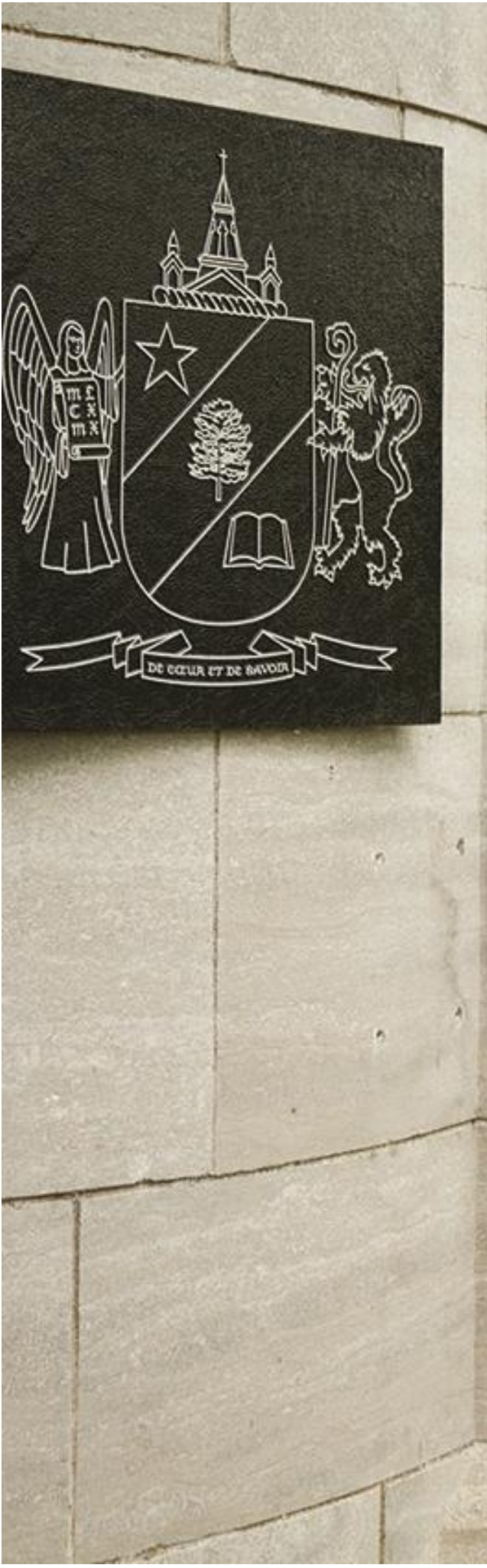




DIRECTIVE DE GOUVERNANCE DE L'INTELLIGENCE ARTIFICIELLE GÉNÉRATIVE

DIRECTION GÉNÉRALE

■ ■ ■ CÉGEP DE SAINT-JÉRÔME
Saint-Jérôme | Mont-Tremblant | Mont-Laurier

Suivi de la directive par le comité de direction	Dates
Adoption : Entrée en vigueur : Modifications :	9 juin 2026 9 juin 2026 18 août 2026 14 septembre 2026

TABLE DES MATIÈRES

PRÉAMBULE.....	4
1. OBJECTIFS.....	4
2. CADRE RÉGLEMENTAIRE	4
3. DÉFINITIONS	5
4. PRINCIPES DIRECTEURS.....	7
Finalité légitime et proportionnée.....	7
Exploration encadrée.....	7
Rigueur, biais et exactitude des résultats.....	7
Inclusion et équité	8
Contrôle humain	8
Transparence et traçabilité	8
Protection des renseignements personnels, confidentiels et sécurité des données.....	8
Responsabilité et correction	9
5. USAGES AUTORISÉS	9
6. USAGES INTERDITS	10
7. ENCADREMENT ET DISCUSSION AVEC LE GESTIONNAIRE	11
8. ACQUISITION DE LICENCE	11
9. FORMATION PRÉALABLE.....	11
10. RÔLES ET RESPONSABILITÉS.....	11
Bureau de l'IAG	11
Comité d'accès à l'information et à la protection des renseignements personnels (CAIPRP)	14
Comité de direction.....	14
Direction des communications et des ressources informationnelles (DCRI)	15
Direction des études (DÉ).....	15
Direction des ressources humaines (DRH)	16
Secrétariat général et affaires juridiques	16
Personnes utilisatrices.....	16
11. DIFFUSION ET MISE À JOUR	17
12. ENTRÉE EN VIGUEUR	18
ANNEXE - ACTIVITÉS DE RECHERCHE	19

PRÉAMBULE

L'émergence de l'intelligence artificielle générative (ci-après nommée « l'IAG ») transforme profondément les pratiques dans les milieux de l'enseignement, de l'administration et des services. Devant ces changements importants, le Cégep de Saint-Jérôme (ci-après nommé « le Collège ») doit s'adapter à cette nouvelle réalité. La mise en place d'une structure de gouvernance de l'IAG devient donc essentielle.

La directive de gouvernance de l'IAG (ci-après nommée « la Directive ») permet d'assurer une utilisation responsable, sécuritaire et éthique de ces technologies, en cohérence avec la mission éducative du Collège, ses valeurs institutionnelles ainsi que les exigences légales et réglementaires applicables. Elle contribue également à maintenir la cohérence, l'éthique et l'équité dans les pratiques au sein du Collège. Concrètement, la Directive vise à clarifier les rôles et responsabilités de chacun, encadrer les usages de manière transparente, protéger les renseignements personnels et les données institutionnelles, et soutenir une utilisation pédagogique et organisationnelle éthique, inclusive, responsable et écoresponsable.

La Directive constitue un document de référence général, duquel d'autres documents d'encadrement découleront afin d'assurer que la gouvernance de l'IAG prenne en compte les différentes réalités institutionnelles, notamment aux niveaux pédagogiques, administratifs et de la recherche, pour lesquels des particularités doivent incontestablement être prises en considération.

1. OBJECTIFS

La Directive vise à doter le Collège d'un cadre structurant, cohérent et évolutif afin d'encadrer l'utilisation de l'IAG dans l'ensemble de ses activités. Le Collège se dotera également d'outils et de processus complémentaires qui lui permettra d'encadrer et d'anticiper les risques, de maximiser les bénéfices pour sa communauté et de favoriser un développement technologique éthique et durable.

2. CADRE RÉGLEMENTAIRE

La Directive s'inscrit notamment dans un contexte régi par :

- La *Charte des droits et libertés de la personne*
- L'Arrêté ministériel no 2025-02 du ministre de la Cybersécurité et du Numérique relatif à l'usage responsable de l'IA au sein des organismes publics

- Le décret G-1.03, incluant ses sections I et II portant sur la gouvernance et la gestion responsable des ressources informationnelles des organismes publics
- La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*
- L'Énoncé de principes pour une utilisation responsable de l'intelligence artificielle par les organismes publics
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (ci-après nommée la « Loi sur l'accès »)
- La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (ci-après nommée la « Loi 25 »)
- La *Loi sur les archives du Québec*
- La Politique sur la sécurité de l'information
- La Directive concernant les règles de gouvernance en matière de protection des renseignements personnels

3. DÉFINITIONS

Cette section définit les notions reliées à l'IAG. Les définitions sont très largement inspirées du lexique de l'Office québécois de la langue française¹.

Biais algorithmique : Tendance prédictive ou générative non désirée d'un système d'intelligence artificielle à favoriser ou à défavoriser certains résultats plutôt que d'autres.

Brèche de sécurité informatique liée à l'IAG : Vulnérabilité informatique ayant permis une intrusion illicite dans un outil ou un système d'IAG et pouvant entraîner le vol, la divulgation ou la destruction de données importantes pour une organisation.

Une brèche de sécurité informatique liée à l'IAG ou un imprévu relié à l'IAG est qualifié comme tout événement non planifié ayant un impact potentiel ou avéré sur :

- La confidentialité ou la sécurité des données
- L'intégrité des résultats fournis par l'outil ou le système IA du Collège (ex. : réponse incomplète, erronée, biaisée)
- L'expérience ou la réputation de l'organisation

¹ Office québécois de la langue française, [L'intelligence artificielle en évolution : les termes de l'IA](#) (page consultée le 11 mai 2026).

Cycle de vie de l'information : L'ensemble des étapes que franchit l'information, de sa conception en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation permanente ou sa destruction, en conformité avec le calendrier de conservation du Collège.

Évaluation des facteurs relatifs à la vie privée (EFVP) : Démarche préventive et structurée visant à identifier, analyser et atténuer les risques que peut poser un projet technologique sur la vie privée des personnes. Elle permet de s'assurer que les mesures de protection appropriées sont intégrées dès la conception et tout au long du cycle de vie du projet.

Hallucination d'IAG : Contenu incorrect, inopportun ou fictif généré par un modèle d'intelligence artificielle et présenté de manière factuelle, comme si les informations étaient authentiques ou en adéquation avec la requête d'origine.

Incident : Événement qui porte atteinte ou qui est susceptible de porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information, ou plus généralement à la sécurité des systèmes d'information, par exemple une interruption des services ou une réduction de leur qualité.

Intelligence artificielle (IA) : Domaine d'étude ayant pour objet l'imitation des facultés cognitives de l'intelligence humaine dans le but de créer des systèmes ou des machines capables d'exécuter des fonctions relevant normalement de celle-ci, ou de les surpasser

IA générative (IAG) : Système d'intelligence artificielle utilisé pour produire du contenu au moyen d'algorithmes et de mégadonnées, généralement sous forme de texte, de son, de vidéo ou d'image (Série de sensibilisation, Gouvernement du Canada, ITSAP.00.041).

IAG privée : Tout outil utilisant l'IAG intégrée dans les infrastructures technologiques privées du Collège et pouvant utiliser de manière automatisée les données internes.

IAG publique : Toute version « grand public » gratuite ou non de système d'IAG, comme les versions en ligne de Copilot et ChatGPT, accessible par le Web à l'extérieur de l'organisation.

IA traditionnelle : L'IA dite traditionnelle regroupe des systèmes conçus pour analyser des données existantes afin de classer, détecter des motifs ou faire des prédictions, sans générer de contenu nouveau. Elle inclut notamment : l'IA analytique et prédictive, l'IA de reconnaissance (image, voix, etc.) et l'IA d'automatisation et d'aide à la décision.

Personne utilisatrice : Toute personne physique ou morale autorisée à utiliser les actifs informationnels et les technologies de l'information du Collège, dans ses locaux ou à distance. Sont considérées comme des personnes utilisatrices les membres du personnel enseignant, du personnel professionnel, du personnel de soutien, du personnel d'encadrement, de la communauté étudiante ainsi que les tiers autorisés.

Renseignement personnel : Conformément à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, renseignement qui concerne une personne physique et qui permet de l'identifier.

4. PRINCIPES DIRECTEURS

Le Collège s'appuie sur les principes établis par le gouvernement du Québec pour l'utilisation responsable de l'IAG dans les organismes publics. Ces principes, publiés par le ministère de la Cybersécurité et du Numérique (ci-après nommé « le MCN »), visent à assurer un développement et une utilisation de l'IAG respectueux des lois, des personnes et de l'intérêt public².

Finalité légitime et proportionnée

Tout usage de l'IAG au sein du Collège doit poursuivre une finalité légitime, nécessaire et proportionnée. La pertinence du recours à l'IAG doit être démontrée au regard des objectifs visés, de la valeur ajoutée attendue et du niveau de risque associé.

Le principe de proportionnalité implique que les efforts d'analyse, d'encadrement et de contrôle soient calibrés en fonction de la sensibilité des données traitées et de l'incidence potentielle du cas d'usage sur les personnes, le Collège ou ses activités.

Exploration encadrée

L'utilisation de l'IAG doit être envisagée comme un outil d'appui, d'innovation et d'efficacité, jamais comme un substitut au jugement professionnel, à l'expertise et à l'analyse humaine ou à la mission du Collège.

Rigueur, biais et exactitude des résultats

Toute information, analyse ou contenu produit à l'aide de l'IAG doit être vérifié, validé et bonifié avant diffusion interne ou externe, en conformité avec les standards du Collège. Il est important de noter que l'utilisation de l'IAG peut introduire des biais dans les résultats obtenus et des hallucinations, soit de l'information fausse ou trompeuse. L'utilisation de résultats provenant de réponses biaisées pourrait fausser des travaux exécutés et encourager des préjugés discriminatoires.

L'essentiel des processus et les tâches qui requièrent traditionnellement l'intelligence et le jugement humains tels que les analyses, les études de cas, la rédaction de documents complexes, doivent demeurer de nature humaine.

² MCN, Énoncé de principes pour une utilisation responsable de l'intelligence artificielle par les organismes publics, édition 2025.

L'exactitude et la qualité de l'information et du contenu diffusés demeurent sous la responsabilité du membre du personnel et des gestionnaires. De plus, toutes les pratiques impliquant l'IAG doivent être en conformité avec l'ensemble des documents normatifs en vigueur.

Les pratiques ayant recours à l'IAG dans un contexte d'enseignement et d'apprentissage doivent être encadrées sur le plan pédagogique, accompagnées d'une sensibilisation aux enjeux de plagiat, faire l'objet d'une validation des résultats et s'inscrire dans une démarche de transparence. Des balises pédagogiques seront notamment développées afin d'assurer le respect de ce principe.

Inclusion et équité

L'utilisation responsable des systèmes d'IAG doit viser à répondre aux besoins de la communauté collégiale, tout en faisant la promotion de la diversité et de l'inclusion. Tout système d'IAG doit minimiser les risques et les inconvénients pour la communauté collégiale et éviter de causer une fracture numérique.

Contrôle humain

Le membre du personnel concerné et sa direction ou son service conservent en tout temps le contrôle et la responsabilité du contenu final. L'IAG ne se substitue pas au jugement, à la sensibilité, ni à la décision humaine. Toute utilisation permise de l'IAG doit faire l'objet des autorisations prévues aux présentes.

Transparence et traçabilité

L'utilisation responsable de l'IAG au Collège doit se faire dans le respect du principe de transparence. Toute personne utilisatrice doit ajouter une indication visible lorsqu'un système d'IAG est employé pour la prestation de services numériques ou pour la génération de contenus institutionnels.

Le Collège recommande l'utilisation de la [Notice d'usage de l'IAG](#) créée par la Fédération des Cégeps.

Protection des renseignements personnels, confidentiels et sécurité des données

Il est strictement interdit de soumettre ou verser dans un outil d'IAG toute information confidentielle, stratégique, personnelle ou non publique, notamment :

- Tout renseignement personnel;

- Documents internes ou projets non diffusés au public contenant des renseignements sensibles ou stratégiques, notamment des actifs intellectuels, des données confidentielles ou des résultats de recherche;
- Données financières, contractuelles ou de ressources humaines;
- Informations relatives aux partenaires non disponibles publiquement;
- Données de recherche (à moins qu'elles aient été anonymisées)³;
- Correspondances (par tout mode de communication), enregistrements ou comptes rendus internes.

Responsabilité et correction

Toute erreur résultant d'une utilisation inadéquate de l'IAG doit être signalée sans délai à la Direction des communications et ressources informationnelles (DCRI), afin de permettre une correction rapide, dans le respect des valeurs de rigueur, d'intégrité et de transparence. Le signalement doit également être effectué auprès du supérieur immédiat.

Lorsque l'incident concerne des renseignements personnels, les mécanismes de signalement d'un incident de confidentialité doivent être suivis, en se référant à la [Directive concernant les règles de gouvernance en matière de protection des renseignements personnels](#).

5. USAGES AUTORISÉS

L'utilisation de l'IAG doit être envisagée comme un outil d'appui, d'innovation et d'efficacité, jamais comme un substitut au jugement professionnel, à l'expertise et à l'analyse humaine ou à la mission du Collège.

L'usage de l'IAG est autorisé dans un cadre professionnel, académique et de recherche, sous supervision humaine et dans le respect des principes directeurs énoncés ci-haut. Les usages suivants sont notamment permis :

- Recherche et analyse d'un document afin d'en comprendre le contenu, le contexte et d'en approfondir l'interprétation, à condition de valider toute donnée et toute information générée par l'IAG de façon indépendante, avant d'utiliser le contenu généré. Il est impératif de valider l'information à partir des sources originales, l'IAG pouvant générer des interprétations ou des conclusions erronées.

³ L'utilisation de l'IAG en recherche fera l'objet d'une annexe qui est en élaboration.

- Aide à la rédaction ou à la révision linguistique (idées, reformulations, traductions, résumés), sous réserve d'une validation humaine complète avant diffusion - **uniquement** dans les situations n'impliquant en aucun cas des renseignements personnels, confidentiels, ou stratégiques.
- Production de supports visuels ou graphiques d'inspiration, à condition de ne pas imiter ni altérer des faits réels et de respecter le droit d'auteur. Tout usage de logos et d'images du Collège doit par ailleurs être validé auprès du Service des communications et du recrutement, conformément à la pratique habituelle d'utilisation d'images libres de droits.
- Génération d'idées, de communication, de formations ou d'activités, en appui aux équipes, mais non en substitution à leur réflexion.
- Production de matériel didactique basé sur des informations publiques et libres de droits - **uniquement** dans les situations n'impliquant en aucun cas des renseignements personnels, confidentiels ou stratégiques.

6. USAGES INTERDITS

Les usages suivants sont formellement prohibés :

- Confier à l'IAG la rédaction intégrale d'un document⁴, de paragraphes, de sections complètes d'un communiqué, d'une analyse, d'une recommandation ou d'un rapport de recherche. **Risques : plagiat, fraude intellectuelle, violation de droit d'auteur.**
- Transmettre à un outil d'IAG des informations confidentielles, sensibles ou protégées. **Risques : violation grave de la Loi sur l'accès, violation des ententes de confidentialité signées par les employés, sanctions administratives et pécuniaires, violation de la confidentialité des données, génération d'un incident de confidentialité.**
- Produire des images, vidéos ou graphiques susceptibles d'induire en erreur ou de dissimuler la réalité. **Risques : diffusion de fausse information, mésinformation.**
- Transcription de réunions ou de rencontres ou production d'un compte rendu à partir d'une transcription. Il est toutefois permis de structurer des notes brèves en un résumé lisible ou un projet de procès-verbal préliminaire. **Risques : vice de consentement, cueillette non autorisée de renseignements personnels, violation de la confidentialité, génération d'un incident de confidentialité.**

⁴ La rédaction intégrale désigne le fait de reprendre intégralement ou en majeure partie, de copier, de changer quelques mots ou d'utiliser un texte tel quel.

7. ENCADREMENT ET DISCUSSION AVEC LE GESTIONNAIRE

Une liste d'applications approuvées est publiée et mise à jour régulièrement par la DCRI. Tout employé qui souhaite adopter ou poursuivre l'utilisation d'un outil qui ne figure pas sur cette liste est invité à en discuter avec son gestionnaire. L'employé devra ensuite consulter le Bureau de l'IAG afin que les analyses requises soient réalisées, dont une analyse de sécurité et de conformité. Cette démarche vise à évaluer le besoin de l'employé, la pertinence de l'outil, à s'assurer de la conformité et de la sécurité des usages envisagés, ainsi qu'à vérifier leur alignement avec les valeurs et les objectifs de l'organisation.

Par ailleurs, tout employé qui éprouve un doute quant à l'interprétation de la présente Directive ou qui a toute autre question est invité à en discuter avec son supérieur immédiat.

8. ACQUISITION DE LICENCE

Toute utilisation d'un logiciel ou d'un système d'IAG impliquant des frais initiaux ou récurrents doit faire l'objet d'une approbation préalable par le gestionnaire et le Comité de direction, à la suite des analyses du Bureau de l'IAG et du CAIPRP. Cette exigence s'applique tant aux usages en cours qu'aux nouvelles initiatives.

9. FORMATION PRÉALABLE

Afin d'assurer une utilisation responsable, sécuritaire et conforme de l'IAG, toute personne utilisatrice souhaitant utiliser ces outils dans le cadre de ses fonctions doit avoir complété le module de sensibilisation de base obligatoire. Ce dernier s'inscrit dans le cadre d'un programme institutionnel de formation et de sensibilisation à l'IAG. La réussite de ce module constitue une condition préalable à l'utilisation d'outils d'IAG dans un contexte professionnel et pourra être exigée dans le cadre des mécanismes de gouvernance et de conformité liés à la Directive.

10. RÔLES ET RESPONSABILITÉS

La présente Directive définit les rôles et les responsabilités de chacun dans la gestion de l'utilisation de l'IAG au Collège.

Bureau de l'IAG

Le Bureau de l'IAG est institué par la présente Directive. Il a pour mandat d'assurer l'accompagnement opérationnel des personnes demanderesse du Collège dans le

développement, l'expérimentation et l'utilisation des systèmes d'IAG. En tenant compte de l'objectif visé des personnes demanderesse, il les conseille et soutient dans la préparation de leur projet tout en leur laissant la responsabilité de préparer et de documenter leur dossier.

Le Bureau de l'IAG a une vision globale des projets existants et peut conseiller les personnes demanderesse sur l'utilisation des outils déjà en place, la nécessité d'ajustements liés à la sécurité ou la conformité, ou sur la faisabilité et la pertinence de leur projet.

De façon plus précise, mais non limitative, les responsabilités du Bureau de l'IAG sont les suivantes :

Accompagnement des personnes demanderesse

- accueillir et guider les personnes demanderesse souhaitant développer ou utiliser un système d'IAG;
- informer les personnes demanderesse des étapes du processus institutionnel et des exigences de gouvernance, tout en leur laissant la responsabilité de la préparation du projet;
- conseiller les personnes demanderesse sur les outils existants : identifier ceux qui sont déjà utilisés ou proposer des équivalents pour éviter la duplication;
- veiller à contacter les personnes demanderesse et leur gestionnaire afin de leur transmettre le résultat de l'analyse de leur projet.

Soutien technique

- fournir un appui pour la réalisation des analyses requises;
- analyser les projets sous les angles juridique et réglementaire, éthique et biais potentiels, de la cybersécurité, de la protection des renseignements personnels et conformité à la Loi 25, des impacts organisationnels;
- maintenir une vue d'ensemble des projets IAG existants pour orienter les nouvelles propositions.

Veille, formation et diffusion des bonnes pratiques

- assurer une veille technologique, réglementaire et éthique sur l'IAG afin de soutenir l'évolution des pratiques au Collège;
- développer et diffuser des guides, outils et bonnes pratiques visant à favoriser une utilisation responsable, sécuritaire et conforme de l'IAG au sein de la communauté collégiale;
- documenter les risques, les enjeux et les bonnes pratiques.

Suivi, audits et amélioration continue

- mettre en place des mécanismes de suivi afin d'assurer une utilisation responsable et sécuritaire des systèmes d'IAG;
- mettre en œuvre un processus de rétroaction permettant aux personnes utilisatrices de signaler les anomalies observées dans les systèmes d'IAG, notamment les hallucinations, les biais ou les résultats erronés;
- coordonner la documentation et l'analyse des incidents ou comportements inattendus des systèmes d'IAG;
- planifier des revues périodiques des systèmes d'IAG afin d'évaluer leur pertinence, leur performance et leurs impacts;
- collaborer avec les directions et services concernés pour réaliser des audits périodiques, notamment en matière de sécurité de l'information, de conformité juridique et réglementaire, de protection des renseignements personnels et de performance et de fiabilité des systèmes;
- recommander les ajustements nécessaires afin d'assurer la robustesse des systèmes d'IAG face aux requêtes erronées ou malveillantes et de favoriser l'amélioration continue;
- assurer une vigie quant à la gestion et le suivi du portefeuille institutionnel des projets d'IAG;
- suivre l'évolution des systèmes d'IAG tout au long de leur cycle de vie;
- assurer la documentation et la cartographie institutionnelle des usages de l'IAG;
- assurer la coordination entre les directions, services et départements impliqués dans les projets d'IAG.

Le Bureau de l'IAG est composé des personnes occupant les fonctions suivantes ou de la personne déléguée au sein de leur direction ou service :

- Analyste spécialisé en informatique au service des ressources des technologies de l'information (SRTI);
- Analyste-conseil spécialisée en affaires juridiques au secrétariat général et affaires juridiques;
- Agente de soutien administratif à la direction des communications et ressources informationnelles;

- Conseiller pédagogique au service du développement pédagogique et à la gestion des programmes;
- Conseiller pédagogique à la direction de la formation continue, service aux entreprises et international;
- Spécialiste en sciences de l'information (plagiat et droit d'auteur) au service des ressources didactiques et à la gestion des programmes.

Comité d'accès à l'information et à la protection des renseignements personnels (CAIPRP)

Le CAIPRP soutient la mise en œuvre de la gouvernance institutionnelle de l'IAG en assurant l'analyse des projets et la formulation de recommandations au Comité de direction. Les responsabilités tactiques et éthiques liées à l'utilisation de l'IAG lui sont confiées, dont notamment les suivantes :

- effectuer des recommandations au Comité de direction quant à l'application de balises d'utilisation de l'IAG, à la priorisation de projets intégrant de l'IAG, ainsi que de tout autre aspect relié à la gouvernance, aux risques, aux enjeux et aux opportunités entourant l'utilisation de l'IAG;
- évaluer les projets d'IAG, prendre connaissance des analyses de risque effectuées par le Bureau de l'IAG et formuler des recommandations au Comité de direction;
- recommander des formations adaptées aux besoins de la communauté collégiale et promouvoir l'amélioration continue des pratiques liées à l'IAG;
- assurer l'application et le suivi de la réglementation ainsi que les bonnes pratiques entourant l'IAG.

Comité de direction

Le Comité de direction est la principale instance décisionnelle du Collège en matière d'IAG. Il lui revient de se positionner quant aux recommandations qui lui sont soumises, en veillant notamment à l'alignement des initiatives d'IAG avec la mission éducative du Collège, son plan stratégique, ses valeurs et les exigences légales et réglementaires auxquelles il est soumis. De façon plus précise, mais non limitative, ses responsabilités sont :

- d'approuver les normes et les cadres de gouvernance applicables aux systèmes d'IAG;
- de recevoir et d'analyser les recommandations du CAIPRP;

- d'approuver ou de refuser le déploiement de tout système d'IAG;
- d'adopter la Directive sur la gouvernance de l'intelligence artificielle générative, ainsi que toute modification à celle-ci.

Chacun des directeurs doit également assurer l'application et le respect de la Directive dans sa direction.

Direction des communications et des ressources informationnelles (DCRI)

La DCRI maintient un registre des cas d'usage de l'IAG. Ce registre consigne les **scénarios d'utilisation autorisés** (et non chaque utilisation individuelle), leur niveau de risque, les données impliquées, le responsable désigné et le statut d'approbation. Il est tenu à jour par la DCRI et révisé périodiquement.

L'inscription d'un nouveau cas d'usage au registre est précédée du processus d'évaluation décrit dans la Directive. Toute personne utilisatrice qui souhaite recourir à un outil d'IAG dans le cadre de ses fonctions doit s'assurer que le scénario envisagé figure parmi les cas d'usage autorisés au registre, ou demander son inscription par la voie prévue.

Direction des études (DÉ)

La DÉ a la responsabilité du volet pédagogique de la gouvernance de l'IAG. À cet égard, elle doit notamment :

- définir la vision institutionnelle pédagogique de l'IAG;
- élaborer les balises d'usage pédagogique et les orientations;
- former et accompagner le personnel enseignant;
- soutenir l'intégration dans les cours et les évaluations;
- développer la littératie IAG chez les personnes étudiantes;
- assurer l'alignement avec l'intégrité intellectuelle (PIÉA, politique institutionnelle d'évaluation des apprentissages);
- coordonner la veille pédagogique.

Direction des ressources humaines (DRH)

La DRH accompagne le Bureau de l'IAG dans le déploiement de tout système d'IAG, au niveau notamment de la formation, de la communication et de la gestion du changement. Elle assure également une appropriation progressive de ces systèmes par chacune des équipes.

Secrétariat général et affaires juridiques

Le Secrétariat général et affaires juridiques agit à titre de responsable de l'accès aux documents du Collège ainsi que de responsable de la protection des renseignements personnels. La personne responsable de la protection des renseignements personnels doit par ailleurs être impliquée dans la configuration et le déploiement de tout système d'IAG.

Personnes utilisatrices

Toute personne utilisatrice des systèmes d'IAG du Collège est responsable de les utiliser de manière éthique, sécurisée, transparente et de protéger les données et informations du Collège dans toutes ses actions.

À cette fin, elle doit :

- prendre connaissance de la présente Directive et des autres documents normatifs qui en découlent ;
- vérifier, valider et bonifier toute information, analyse ou contenu produit à l'aide de l'IAG avant toute diffusion interne ou externe, en conformité avec les standards Collège;
- ajouter une indication visible lorsqu'un système d'IAG est employé pour la prestation de services numériques ou pour la génération de contenus institutionnels;
- maintenir la nature humaine de l'essentiel des processus et des tâches qui requièrent traditionnellement l'intelligence et le jugement humains, tel que les analyses, les études de cas et la rédaction de documents complexes;
- veiller à ce que l'exactitude et la qualité de l'information et du contenu diffusés demeurent sous la responsabilité du membre du personnel. S'assurer également que toutes les pratiques impliquant l'IA respectent l'ensemble des lois, règlements, politiques et autres documents normatifs applicables en vigueur;
- conserver en tout temps le contrôle et la responsabilité du contenu final, veiller à ce que l'IAG ne se substitue pas au jugement, à la sensibilité, ni à la décision humaine. Toute utilisation permise de l'IAG doit faire l'objet des autorisations prévues aux présentes;

- éviter de soumettre ou de verser dans un outil d'IAG toute information confidentielle, stratégique, personnelle ou non publique, notamment :
 - tout renseignement personnel;
 - documents internes ou projets non diffusés au public contenant des renseignements sensibles ou stratégiques, notamment des actifs intellectuels, des données confidentielles ou des résultats de recherche;
 - données financières, contractuelles ou de ressources humaines;
 - informations relatives aux partenaires non disponibles publiquement;
 - données de recherche (à moins qu'elles aient été anonymisées)⁵;
 - correspondances (par tout mode de communication), enregistrements ou comptes rendus internes.
- utiliser les systèmes d'IAG qui sont mis à sa disposition uniquement aux fins auxquelles ils sont destinés ;
- signaler tout incident résultant d'une utilisation inadéquate de l'IAG sans délai à son supérieur immédiat ou son enseignant afin de permettre une correction rapide, dans le respect des principes directeurs de la Directive. Lorsque l'incident concerne des renseignements personnels, les mécanismes de signalement habituels applicables à ce type de situation doivent être suivis⁶;
- collaborer à toute intervention visant à indiquer ou à mitiger une menace à la sécurité de l'information ou une brèche informatique liée à l'IAG ;
- respecter la *Loi sur le droit d'auteur* et les principes d'intégrité intellectuelle (citer ses sources, ne pas plagier, etc.) lors de l'utilisation des systèmes d'IAG;
- discuter avec son supérieur immédiat en cas de doute quant à l'interprétation de la Directive ou pour toute autre question.

11. DIFFUSION ET MISE À JOUR

La Direction générale est responsable de la diffusion et de la mise à jour de la Directive. Cette dernière sera révisée annuellement ou au besoin.

⁵ L'utilisation de l'IAG en recherche fera l'objet d'une annexe qui est en élaboration.

⁶ [Directive concernant les règles de gouvernance en matière de protection des renseignements personnels](#)

12. ENTRÉE EN VIGUEUR

La Directive entre en vigueur dès son adoption par le comité de direction. Une fois adoptée, d'autres documents d'encadrement découleront des travaux des différentes instances.

ANNEXE - ACTIVITÉS DE RECHERCHE

À venir.