
TITRE : TIC-04 : Utilisation responsable de l'intelligence artificielle

CATÉGORIE : 08-Technologies

EN VIGUEUR : 2026-09-29

RÉVISÉE : Sans objet

1. OBJET

La présente directive administrative est mise en œuvre conformément à la Méta-directive ADM-01 – *Élaboration, révision et adoption d'une directive administrative*. Elle découle des limites opérationnelles de la direction de l'éducation 3.3 – *Traitement des parents, tuteurs et des élèves*, 3.4 – *Traitement du personnel et des bénévoles* et 3.6 – *Protection des actifs*, à ce titre, fait l'objet d'un rapport annuel de monitoring.

La présente directive administrative établit les exigences encadrant l'acquisition, l'autorisation et l'utilisation de systèmes d'intelligence artificielle dans les activités pédagogiques, administratives et opérationnelles du Conseil scolaire catholique des Grandes Rivières, ci-après appelé le CSCDGR ou le Conseil.

Elle vise à favoriser une utilisation responsable, éthique, sécuritaire, transparente et équitable de l'intelligence artificielle au service de la réussite, du bien-être et de l'engagement des élèves, de la qualité des services et de l'efficacité organisationnelle.

Toute utilisation de l'intelligence artificielle au CSCDGR doit respecter la dignité humaine, protéger les renseignements personnels, préserver le jugement et la responsabilité de la personne, soutenir la mission de l'éducation catholique de langue française et tenir compte des risques de biais, d'erreur, d'atteinte aux droits de la personne et de cybersécurité.

Toute utilisation de l'intelligence artificielle au CSCDGR doit respecter la dignité de chaque personne, les droits de la personne, la vie privée, l'intégrité scolaire, la propriété intellectuelle et les règles de sécurité de l'information. Elle doit également tenir compte des limites des outils utilisés, notamment du risque que les résultats générés soient inexacts, incomplets, trompeurs, biaisés ou inappropriés au contexte.

L'intelligence artificielle constitue un outil de soutien. Elle ne remplace pas le jugement professionnel, la réflexion critique, la responsabilité décisionnelle, l'intervention humaine, ni les processus d'approbation établis par le Conseil.

2. DESTINATAIRES

2.1. La présente directive administrative s'adresse :

- aux membres du personnel du Conseil, sans égard à leur fonction, à leur statut ou à leur lieu de travail;
- aux élèves;

- aux parents, tutrices et tuteurs lorsqu'ils accompagnent un élève dans l'utilisation d'un outil d'intelligence artificielle fourni, recommandé ou autorisé par le Conseil;
 - aux bénévoles, stagiaires, consultants, fournisseurs, partenaires et à toute autre personne autorisée à accéder aux systèmes, aux réseaux, aux ressources, aux renseignements ou aux données du CSCDGR;
 - aux fournisseurs qui conçoivent, offrent, intègrent, hébergent, exploitent, entretiennent ou soutiennent un système ou un service intégrant des fonctions d'intelligence artificielle destiné au CSCDGR.
- 2.2. Toute personne visée par la présente directive doit connaître et respecter les responsabilités qui s'appliquent à son rôle. Les gestionnaires, les directions d'école et les personnes responsables de la supervision veillent à ce que les personnes sous leur responsabilité reçoivent l'information, l'encadrement et l'accompagnement nécessaires.

3. DÉFINITIONS

« **Apprentissage automatique** (Machine Learning) » se définit comme une branche de l'IA reposant sur la conception d'algorithmes qui rendent les systèmes capables d'apprendre à partir de données et d'améliorer ainsi leurs performances sans être explicitement programmés.

« **Apprentissage profond** (ou Deep Learning) » se définit comme une sous-catégorie de l'apprentissage automatique qui utilise des réseaux de neurones artificiels à plusieurs couches pour analyser des données complexes et extraire des représentations hiérarchiques.

« **Biais** » se définit comme une tendance systématique susceptible de produire des résultats inexacts, inéquitables ou discriminatoires à l'égard d'une personne ou d'un groupe.

« **Décision automatisée** » se définit comme une décision prise entièrement ou principalement au moyen d'un système automatisé, sans examen humain suffisant.

« **Donnée institutionnelle** » se définit comme tout renseignement, document ou contenu détenu, créé, reçu ou géré par le CSCDGR dans le cadre de ses activités.

« **Données personnelles** » se définit comme des informations propres à un individu et permettant de l'identifier.

« **Incident lié à l'intelligence artificielle** » se définit comme toute situation réelle ou présumée pouvant compromettre la confidentialité, l'intégrité ou la disponibilité des renseignements ou des systèmes, porter atteinte aux droits d'une personne, produire un résultat préjudiciable ou constituer une utilisation non conforme d'un outil d'intelligence artificielle.

« **Intelligence artificielle (IA)** » se définit comme un domaine de l'informatique visant à créer des systèmes capables d'effectuer des tâches qui nécessitent normalement l'intelligence humaine, comme : apprendre, raisonner, résoudre des problèmes, percevoir et comprendre le langage.

« **Intelligence artificielle générative** » se définit comme un type d'intelligence artificielle qui utilise des modèles capables de créer du contenu original (texte, images, audio, vidéo, code, etc.) en apprenant à partir de grandes quantités de données existantes. À noter : L'IA générative ne fait pas qu'analyser ou classer des données; elle génère de nouvelles informations qui imitent ou innovent par rapport aux données d'entraînement.

« **Outil autorisé** » se définit comme un système d'intelligence artificielle ayant fait l'objet d'une évaluation et d'une approbation par le Service informatique, en collaboration avec les services concernés, conformément au processus prévu dans la présente directive.

« **Réidentification** » se définit comme un processus par lequel on parvient à retrouver l'identité d'une personne à partir de données préalablement anonymisées ou présentées sous des pseudonymes.

« **Renseignement confidentiel** » se définit comme un renseignement qui n'est pas du domaine public et dont l'accès est limité aux personnes autorisées en raison de leurs fonctions.

« **Renseignement personnel** » se définit comme tout renseignement permettant d'identifier une personne directement ou indirectement, notamment les renseignements scolaires, médicaux, disciplinaires, financiers, professionnels ou relatifs à l'emploi.

4. MODALITÉS D'APPLICATION

4.1. Principes directeurs

L'utilisation de l'intelligence artificielle (IA) au CSCDGR repose sur les principes suivants :

4.1.1. Primauté de la personne et responsabilité humaine

L'intelligence artificielle est utilisée comme outil de soutien. Elle ne remplace pas le jugement professionnel, la réflexion critique, la responsabilité individuelle, l'intervention humaine, ni les mécanismes d'approbation établis par le Conseil.

Toute décision ayant un effet sur les droits, les services, le cheminement scolaire, l'évaluation, l'emploi, les conditions de travail, la sécurité ou le bien-être d'une personne doit faire l'objet d'un examen humain significatif. Elle ne peut être prise uniquement à partir d'un résultat, d'une recommandation, d'une prédiction ou d'une analyse générée par un outil d'intelligence artificielle.

La personne qui utilise un résultat généré par l'intelligence artificielle demeure responsable de son contenu, de sa pertinence, de sa qualité et de ses effets.

4.1.2. Valeur pédagogique et organisationnelle ajoutée

Le recours à l'intelligence artificielle doit répondre à une finalité pédagogique, administrative, professionnelle ou opérationnelle claire, légitime et liée au mandat du Conseil.

L'utilisation doit apporter une valeur ajoutée démontrable, notamment en contribuant :

- À la réussite, au bien-être, à l'engagement ou au développement intégral des élèves;

- à la différenciation pédagogique et à l'accessibilité des apprentissages;
- à l'amélioration de la qualité, de la cohérence ou de l'efficacité des services;
- à la réduction de tâches répétitives ou à faible valeur ajoutée;
- au développement professionnel et à l'amélioration continue des pratiques.

L'intelligence artificielle ne doit pas être utilisée lorsqu'une méthode moins intrusive, plus fiable ou mieux adaptée permet d'atteindre raisonnablement le même objectif.

4.1.3. Transparence, prudence et responsabilité

Les usages de l'intelligence artificielle doivent être connus, compris et expliqués aux personnes concernées.

Le niveau d'encadrement, de validation et de surveillance doit être proportionnel aux risques associés à l'utilisation envisagée.

Une vigilance accrue est requise lorsque l'utilisation concerne notamment :

- Des élèves mineurs;
- des renseignements personnels ou confidentiels;
- des personnes ou des groupes susceptibles de subir un préjudice;
- une décision pouvant avoir des conséquences importantes;
- l'évaluation du rendement scolaire ou professionnel;
- la santé, la sécurité ou le bien-être;
- le profilage, la prédiction ou la catégorisation d'une personne;
- la création de contenu susceptible d'être interprété comme une communication officielle du Conseil.

Lorsqu'un doute raisonnable existe quant à la conformité, à la sécurité ou aux effets d'une utilisation, la personne s'abstient d'utiliser l'outil et demande conseil à son superviseur ou au service responsable.

4.1.4. Protection des données et respect de la vie privée

Toute utilisation de l'intelligence artificielle doit respecter la législation applicable ainsi que les politiques, les directives administratives, les procédures et les mesures de sécurité du Conseil.

La personne utilisatrice doit limiter les renseignements traités à ce qui est strictement nécessaire à la finalité autorisée. Elle privilégie, lorsque cela est possible, des données anonymisées, agrégées, fictives ou dépersonnalisées.

L'autorisation d'un outil ne constitue pas une autorisation générale d'y saisir tout renseignement. Les renseignements personnels, confidentiels ou institutionnels ne peuvent être traités que lorsque cet usage précis a été autorisé et que les mesures de protection applicables sont respectées.

4.1.5. Équité, inclusion et prévention des biais

Les outils d'intelligence artificielle doivent être utilisés de manière à prévenir la discrimination, l'exclusion et les effets inéquitables.

Tout résultat susceptible d'influencer une personne, un groupe, une décision ou un service doit faire l'objet d'un examen critique afin de repérer notamment :

- Les biais ou les stéréotypes;
- les omissions importantes;
- les généralisations abusives;
- les obstacles à l'accessibilité;
- les effets différenciés sur certaines personnes ou certains groupes;
- les contenus incompatibles avec les droits de la personne ou les valeurs du Conseil.

Un résultat jugé biaisé, discriminatoire, offensant, trompeur ou préjudiciable ne doit pas être utilisé, diffusé ou conservé comme fondement d'une décision.

4.1.6. Fiabilité, exactitude et validation

Les résultats générés par l'intelligence artificielle ne doivent pas être présumés exacts, complets ou fiables.

Avant d'utiliser, de communiquer ou de publier un résultat généré, la personne utilisatrice doit :

- Vérifier les faits, les chiffres, les citations, les références et les sources;
- confirmer que le contenu correspond au contexte et à la finalité recherchée;
- corriger les erreurs, les omissions, les incohérences et les formulations trompeuses;
- s'assurer que le contenu respecte les exigences légales, professionnelles, pédagogiques et organisationnelles;
- obtenir les approbations requises lorsque le contenu est destiné à une communication officielle ou à une décision.

Le niveau de vérification doit être plus rigoureux lorsque le contenu porte sur une question juridique, financière, médicale, disciplinaire, scolaire, professionnelle ou susceptible d'entraîner un préjudice.

4.1.7. Respect de la propriété intellectuelle et de l'intégrité

L'utilisation de l'intelligence artificielle doit respecter les droits d'auteur, les licences, les conditions d'utilisation, la propriété intellectuelle, la confidentialité et les règles d'attribution des sources.

Il est interdit d'utiliser l'intelligence artificielle pour :

- Reproduire, transformer ou diffuser du contenu protégé sans autorisation;

- présenter comme une production originale un contenu généré ou substantiellement transformé par l'intelligence artificielle lorsque cette présentation contrevient aux attentes établies;
- falsifier une source, une référence, une preuve, une signature, une identité ou une communication;
- contourner une exigence d'apprentissage, d'évaluation, d'approbation ou de reddition de comptes.

4.1.8. Bien-être et équilibre numérique

Le recours à l'intelligence artificielle doit demeurer réfléchi, proportionné et respectueux du bien-être des élèves et du personnel.

Son utilisation ne doit pas :

- Diminuer indûment les interactions humaines nécessaires;
- créer une dépendance excessive à un outil numérique;
- réduire les occasions de réflexion, de créativité, de collaboration ou d'apprentissage actif;
- augmenter inutilement la surveillance, la charge cognitive ou la pression exercée sur une personne;
- nuire à l'autonomie professionnelle ou au développement des compétences.

4.2. Usages autorisés de l'intelligence artificielle (IA)

L'intelligence artificielle peut être utilisée lorsque l'outil et l'usage envisagé sont autorisés par le Conseil, que la finalité est légitime et que les principes et conditions prévus dans la présente directive sont respectés.

L'autorisation d'un outil n'autorise pas automatiquement toutes ses fonctions ni tous les types de renseignements qui pourraient y être traités.

4.2.1. Usages pédagogiques

L'intelligence artificielle peut notamment servir à :

- Soutenir la planification de l'enseignement et de l'apprentissage;
- proposer des pistes de différenciation pédagogique;
- adapter le niveau de langue, le format ou la présentation d'une ressource;
- créer des exemples, des exercices, des questions ou des scénarios destinés à être révisés par le personnel;
- soutenir l'évaluation formative et la rétroaction descriptive, sans remplacer le jugement professionnel;
- favoriser l'accessibilité et l'inclusion;
- soutenir le développement de la pensée critique, de la littératie numérique et de la citoyenneté numérique;

- appuyer l'apprentissage du français et la création de ressources pertinentes au contexte francophone;
- soutenir le développement professionnel du personnel.

4.2.2. Usages administratifs et professionnels

L'intelligence artificielle peut notamment servir à :

- Soutenir la rédaction, la révision, la reformulation, la traduction ou la synthèse d'un document;
- préparer une ébauche, un plan, une liste de vérification ou un outil de travail;
- résumer des renseignements que la personne est autorisée à consulter et à traiter;
- analyser des données anonymisées, dépersonnalisées ou agrégées;
- soutenir la planification, l'organisation du travail et l'amélioration de processus;
- générer des idées, des options ou des pistes de réflexion;
- appuyer la préparation de communications internes ou externes;
- soutenir des tâches techniques, informatiques ou documentaires autorisées.

Toute production destinée à représenter la position officielle du Conseil doit être révisée, validée et approuvée conformément aux processus habituels.

4.2.3. Conditions applicables

Toute utilisation autorisée doit respecter les conditions suivantes :

- L'outil figure parmi les outils autorisés par le Conseil;
- la personne utilise son compte professionnel ou scolaire lorsque cela est exigé;
- l'utilisation respecte les conditions d'âge et les modalités établies par le fournisseur et le Conseil;
- seuls les renseignements nécessaires et permis sont saisis ou téléversés;
- le résultat généré fait l'objet d'une vérification appropriée;
- l'utilisation respecte les droits d'auteur, la propriété intellectuelle et les règles d'attribution;
- toute erreur, tout risque ou tout incident est signalé au superviseur immédiat et conformément au processus établi;
- la personne demeure responsable du contenu qu'elle utilise, adapte, approuve ou communique.

4.3. Usages interdits ou soumis à une autorisation particulière

4.3.1. Usages interdits

Il est interdit :

- D'utiliser un outil d'intelligence artificielle non autorisé dans le cadre des activités du Conseil;
- de saisir, téléverser, divulguer ou traiter des renseignements personnels, confidentiels ou institutionnels dans un outil non autorisé;
- de fournir à un outil des mots de passe, des codes d'accès, des clés de sécurité ou d'autres renseignements permettant d'accéder aux systèmes du Conseil;
- d'utiliser l'intelligence artificielle pour usurper l'identité d'une personne ou créer un contenu trompeur présenté comme authentique;
- de produire ou de diffuser du contenu discriminatoire, haineux, menaçant, harcelant, diffamatoire, violent, frauduleux ou contraire au code de conduite;
- de créer ou de modifier l'image, la voix ou la représentation d'une personne identifiable sans l'autorisation requise;
- d'utiliser l'intelligence artificielle pour contourner une mesure de cybersécurité, une restriction d'accès ou un contrôle institutionnel;
- d'utiliser un résultat généré sans l'avoir vérifié lorsqu'il sert à informer une décision, une communication officielle ou une activité d'apprentissage;
- de présenter comme entièrement personnel ou original un travail généré par l'intelligence artificielle lorsque cette présentation contrevient aux attentes établies;
- d'utiliser l'intelligence artificielle pour surveiller secrètement une personne ou tirer des conclusions sur ses caractéristiques, ses comportements, ses intentions ou son état;
- d'autoriser un outil externe à utiliser les renseignements ou les contenus du Conseil pour entraîner un modèle, sauf lorsque cette utilisation a été expressément approuvée;
- d'effectuer un usage incompatible avec la mission, les valeurs, les politiques, les directives administratives ou les obligations légales du Conseil.

4.3.2. Usages exigeant une autorisation particulière

Une autorisation institutionnelle préalable est requise avant d'utiliser l'intelligence artificielle pour :

- Analyser, évaluer, classer, profiler ou comparer des personnes;

- soutenir une décision relative à l'admission, à l'évaluation, à la discipline, aux services à l'élève, à l'emploi, à la santé, à la sécurité ou aux conditions de travail;
- traiter des renseignements personnels, confidentiels ou sensibles, même dans un outil autorisé, lorsque cet usage n'a pas déjà été expressément approuvé;
- intégrer un outil d'intelligence artificielle à un système, à une application, à un site Web ou à un processus institutionnel;
- automatiser une communication, une recommandation ou une décision destinée à une personne;
- enregistrer, transcrire, résumer ou analyser une rencontre, une conversation ou une communication comportant des renseignements personnels ou confidentiels;
- créer un compte d'élève ou exiger l'utilisation d'un service externe;
- mener un projet pilote, une expérimentation ou une recherche utilisant des données du Conseil;
- créer un agent automatisé destiné à interagir avec des élèves, des parents, des membres du personnel ou le public;
- utiliser une fonction nouvelle ou substantiellement modifiée qui n'a pas encore été évaluée par le Conseil.

L'autorisation peut prévoir des limites concernant les utilisateurs, les finalités, les données, les fonctions, la durée, le nombre de personnes visées et les mesures de surveillance. Elle peut être suspendue ou retirée lorsqu'un risque, un incident, une modification technologique ou une nouvelle exigence le justifie.

4.4. Utilisation personnelle

L'utilisation personnelle d'un outil d'intelligence artificielle est distincte de l'utilisation professionnelle ou scolaire. Elle ne doit jamais comprendre des renseignements personnels, confidentiels ou institutionnels du Conseil, ni être présentée comme une activité autorisée ou approuvée par celui-ci.

L'utilisation d'un appareil personnel, d'un compte personnel ou d'un réseau externe pour accomplir une tâche liée au Conseil demeure assujettie à la présente directive.

5. PROCESSUS

5.1. Évaluation et autorisation des outils d'intelligence artificielle

5.1.1. Demande d'évaluation

Tout outil intégrant des fonctions d'intelligence artificielle doit faire l'objet d'une évaluation avant son acquisition, son activation, son intégration, son déploiement ou son utilisation dans le cadre des activités du CSCDGR.

La demande d'évaluation est transmise au Service informatique par la direction d'école, la direction de service ou la personne responsable du service concerné.

La demande doit notamment préciser :

- La finalité pédagogique, administrative, professionnelle ou opérationnelle recherchée;
- les personnes appelées à utiliser l'outil;
- les personnes susceptibles d'être touchées par son utilisation;
- les fonctions d'intelligence artificielle qui seraient utilisées;
- les catégories de renseignements ou de données susceptibles d'être traitées;
- les avantages attendus;
- les risques connus ou anticipés;
- la durée, la portée et les coûts prévus;
- les mesures d'accompagnement, de formation et de surveillance envisagées.

Aucun projet pilote, essai, abonnement, intégration ou déploiement ne doit être entrepris avant que les autorisations requises aient été obtenues.

5.1.2. Coordination de l'évaluation

Le Service informatique coordonne l'évaluation de l'outil en collaboration avec les services concernés.

Selon la nature de l'usage proposé, l'évaluation peut notamment faire appel :

- Aux Services pédagogiques;
- aux Services à l'élève;
- au Service des ressources humaines et de la paie;
- aux Services financiers;
- au Service des communications et de l'imputabilité;
- à la personne responsable de l'accès à l'information et de la protection de la vie privée;
- à toute autre personne ayant une expertise pertinente.

5.1.3. Critères d'évaluation

L'évaluation porte notamment sur :

- La conformité aux lois, aux règlements, aux directives ministérielles ainsi qu'aux politiques et directives administratives du Conseil;
- la finalité, la nécessité et la proportionnalité de l'utilisation;
- la valeur pédagogique, administrative ou organisationnelle attendue;
- les conditions d'utilisation et les politiques de confidentialité du fournisseur;

- les catégories de renseignements recueillis, utilisés, communiqués, conservés ou supprimés;
- le lieu d'hébergement et de traitement des données;
- l'utilisation éventuelle des données ou des contenus pour entraîner ou améliorer un modèle;
- les mécanismes d'authentification, de contrôle d'accès, de journalisation, de conservation et de suppression;
- les risques en matière de cybersécurité, de confidentialité et de réidentification;
- la fiabilité, l'exactitude, l'explicabilité et les limites connues de l'outil;
- les risques de biais, de discrimination ou d'effets inévitables;
- l'accessibilité, la qualité linguistique et la pertinence pour le contexte francophone catholique;
- les exigences d'âge, de consentement et de création de comptes;
- les recours offerts aux personnes touchées;
- la capacité du Conseil à suspendre l'utilisation, à retirer les accès et à récupérer ou supprimer les données;
- les coûts, les conditions de renouvellement et la dépendance envers le fournisseur.

5.1.4. Décision

À la suite de l'évaluation, l'outil ou l'usage proposé peut être :

- Autorisé;
- autorisé sous conditions;
- autorisé pour un projet pilote limité;
- retourné pour obtenir des renseignements ou des mesures supplémentaires;
- refusé;
- suspendu ou retiré.

L'autorisation précise, selon le cas :

- Les personnes ou les groupes autorisés;
- les finalités permises;
- les fonctions pouvant être utilisées;
- les catégories de renseignements pouvant être traitées;
- les mesures de protection requises;
- les exigences en matière de supervision, de formation et de documentation;

- la durée de l'autorisation;
- les conditions de réévaluation.

L'autorisation d'un outil n'autorise pas tous ses usages. Toute utilisation doit respecter la finalité approuvée et les conditions établies.

5.1.5. Réévaluation

Un outil autorisé doit être réévalué lorsque survient notamment :

- Une modification importante de ses fonctions;
- un changement aux conditions d'utilisation ou à la politique de confidentialité;
- une modification des pratiques de collecte, d'hébergement, de conservation ou d'utilisation des données;
- un incident ou un risque nouveau;
- une modification législative, réglementaire ou ministérielle;
- une utilisation différente de celle qui avait été autorisée;
- un doute quant à sa conformité, à sa sécurité, à sa fiabilité ou à sa pertinence.

Le Conseil peut suspendre ou retirer une autorisation en tout temps lorsqu'il existe un risque pour les personnes, les renseignements, les systèmes, les activités ou la réputation du Conseil.

5.2. Rôles et responsabilités

La mise en œuvre de la présente directive repose sur une responsabilité partagée et complémentaire. Chaque personne et chaque secteur exerce ses responsabilités selon son mandat, ses fonctions et son niveau d'autorité.

5.2.1. Direction de l'éducation et secrétaire-trésorière ou secrétaire-trésorier

La direction de l'éducation et secrétaire-trésorière ou secrétaire-trésorier :

- Assure la mise en œuvre, la coordination et l'évaluation de la présente directive;
- établit les orientations institutionnelles relatives à l'utilisation de l'intelligence artificielle;
- veille à ce que les responsabilités et les mécanismes de contrôle soient clairement établis;
- s'assure que les ressources, la formation et l'accompagnement nécessaires sont offerts;
- autorise, lorsque requis, les usages présentant un niveau de risque élevé ou une portée institutionnelle;
- s'assure du suivi des incidents importants et de la mise en œuvre des mesures correctives;

- rend compte de l'application de la présente directive dans le cadre des mécanismes de monitoring applicables.

5.2.2. Service informatique

Le Service informatique :

- Coordonne l'évaluation technique, technologique et sécuritaire des outils;
- maintient la liste des outils et des usages autorisés;
- établit les conditions techniques d'utilisation, d'accès, d'intégration et de sécurité;
- configure les outils afin de limiter les fonctions et les accès selon les autorisations accordées;
- veille à la protection de la confidentialité, de l'intégrité et de la disponibilité des systèmes et des données;
- encadre l'intégration d'outils d'intelligence artificielle à l'environnement numérique du Conseil;
- limite l'utilisation non autorisée des renseignements et des contenus du Conseil par des fournisseurs externes;
- assure une veille technologique et ajuste les mesures de protection selon l'évolution des risques;
- soutient les membres du personnel dans l'utilisation sécuritaire des outils autorisés;
- reçoit, analyse et prend en charge les incidents liés aux systèmes, aux accès, aux données ou à la cybersécurité;
- documente les incidents et les mesures techniques mises en œuvre;
- collabore avec les autres services aux activités de sensibilisation et de formation.

5.2.3. Personne responsable de l'accès à l'information et de la protection de la vie privée

La personne responsable de l'accès à l'information et de la protection de la vie privée :

- Conseille les services quant aux exigences relatives à la collecte, à l'utilisation, à la communication, à la conservation et à la suppression des renseignements personnels;
- contribue à l'évaluation des outils ou des usages comportant des renseignements personnels, confidentiels ou sensibles;
- vérifie l'application des principes de nécessité, de proportionnalité et de minimisation des renseignements;

- conseille le Conseil sur les avis, les consentements, les évaluations des facteurs relatifs à la vie privée et les mesures de transparence pouvant être requis;
- participe à l'évaluation et à la gestion des atteintes réelles ou présumées à la vie privée;
- détermine, avec les responsables concernés, les obligations de communication, de notification, de conservation et de suivi.

5.2.4. Services pédagogiques et Services à l'élève

Les Services pédagogiques et les Services à l'élève, selon leurs responsabilités respectives :

- Évaluent la pertinence pédagogique et éducative des usages proposés;
- veillent à l'alignement avec les programmes-cadres, les orientations ministérielles, les pratiques d'évaluation et les besoins des élèves;
- soutiennent les écoles dans l'intégration responsable de l'intelligence artificielle;
- élaborent ou recommandent des ressources, des pratiques exemplaires et des activités de formation;
- favorisent le développement de la pensée critique, de la littératie numérique et du discernement éthique;
- veillent à ce que les usages favorisent l'inclusion, l'accessibilité et le respect des besoins particuliers;
- contribuent à l'analyse des risques de biais, de discrimination ou d'effets inévitables;
- s'assurent que les usages proposés soutiennent la mission catholique de langue française du Conseil.

5.2.5. Services administratifs

Les services administratifs :

- Utilisent uniquement des outils et des usages autorisés;
- précisent la finalité de l'utilisation avant de traiter des renseignements;
- limitent les renseignements utilisés à ce qui est nécessaire;
- privilégient les données anonymisées, dépersonnalisées, agrégées ou fictives lorsque possible;
- vérifient et approuvent les contenus générés avant leur utilisation ou leur diffusion;
- respectent les processus d'approbation applicables aux communications, aux décisions et aux documents officiels;
- documentent les usages présentant un risque ou ayant une incidence sur les services, les droits ou les intérêts d'une personne;

- signalent sans délai tout incident, toute erreur importante ou tout usage non conforme;
- collaborent avec le Service informatique et les autres services concernés.

Les gestionnaires administratifs veillent à l'application de la présente directive au sein de leurs équipes.

5.2.6. Service des communications et de l'imputabilité

Le Service des communications et de l'imputabilité :

- Conseille les services sur l'utilisation de contenus générés dans les communications officielles;
- révisé, lorsque requis, les communications destinées au public, aux médias ou à l'ensemble de la communauté scolaire;
- veille à la cohérence des communications avec l'identité, la mission et les valeurs du Conseil;
- coordonne toute communication externe liée à un incident important;
- contribue à établir les attentes de transparence relatives aux contenus générés ou transformés par l'intelligence artificielle.

5.2.7. Directions d'école et directions de service

Les directions d'école et les directions de service :

- Veillent à l'application de la présente directive dans leur secteur;
- s'assurent que les membres du personnel connaissent les outils et les usages autorisés;
- établissent des attentes claires quant à l'utilisation de l'intelligence artificielle;
- approuvent les demandes relevant de leur autorité avant leur transmission aux services responsables;
- s'assurent que les membres du personnel reçoivent la formation et l'accompagnement nécessaires;
- exercent une surveillance proportionnelle aux risques;
- interviennent lorsqu'un usage est non conforme ou susceptible de causer un préjudice;
- signalent sans délai les incidents et collaborent à leur gestion;
- conservent, lorsque requis, les documents permettant de démontrer la conformité de l'utilisation.

5.2.8. Membres du personnel œuvrant auprès des élèves

Les membres du personnel œuvrant auprès des élèves :

- Encadrent explicitement l'utilisation de l'intelligence artificielle dans les activités d'apprentissage;

- précisent aux élèves les usages permis, attendus ou interdits;
- sélectionnent uniquement des outils et des usages autorisés;
- adaptent l'encadrement à l'âge, au niveau scolaire, aux besoins et au degré d'autonomie des élèves;
- enseignent aux élèves à vérifier l'exactitude, la fiabilité, les biais et les sources des contenus générés;
- informent les élèves des attentes en matière d'intégrité scolaire et d'attribution;
- protègent les renseignements personnels et scolaires;
- n'exigent pas la création d'un compte personnel sur un outil non autorisé;
- mettent en œuvre des pratiques d'évaluation qui permettent de vérifier les apprentissages réels de l'élève;
- valorisent le processus, la progression, la réflexion et la démonstration des apprentissages;
- interviennent lorsqu'un usage compromet l'intégrité scolaire, la sécurité ou le bien-être;
- signalent toute situation à risque ou tout incident.

5.2.9. Élèves

Les élèves :

- Utilisent l'intelligence artificielle uniquement lorsqu'elle est autorisée et selon les consignes reçues;
- respectent les conditions d'âge, d'accès et d'utilisation;
- protègent leurs renseignements personnels et ceux des autres;
- ne saisissent ni ne téléversent de renseignements personnels, confidentiels ou scolaires, sauf autorisation explicite;
- vérifient l'exactitude et la pertinence des résultats générés;
- indiquent leur utilisation de l'intelligence artificielle lorsque l'activité ou le membre du personnel l'exige;
- présentent un travail qui démontre leur compréhension et leur appropriation des apprentissages;
- respectent les règles d'intégrité scolaire, les droits d'auteur et les règles d'attribution;
- ne se servent pas de l'intelligence artificielle pour contourner une activité, une évaluation ou une mesure de sécurité;
- signalent au membre du personnel toute situation préoccupante, tout contenu inapproprié ou toute divulgation involontaire de renseignements.

5.2.10. Parents, tutrices et tuteurs

Les parents, tutrices et tuteurs :

- Prennent connaissance des attentes communiquées par l'école;
- soutiennent leur enfant dans une utilisation responsable, sécuritaire et critique de l'intelligence artificielle;
- respectent les conditions d'utilisation et les mesures de protection applicables;
- communiquent avec l'école lorsqu'une préoccupation concerne l'utilisation d'un outil par leur enfant;
- signalent toute situation susceptible de compromettre la sécurité, la vie privée, le bien-être ou l'intégrité scolaire.

5.2.11. Fournisseurs, consultants, partenaires, stagiaires et bénévoles

Les fournisseurs, les consultants, les partenaires, les stagiaires et les bénévoles :

- Respectent la présente directive et les conditions contractuelles applicables;
- utilisent uniquement les outils, les comptes et les accès autorisés;
- protègent les renseignements et les ressources du Conseil;
- n'utilisent pas les renseignements ou les contenus du Conseil pour entraîner un modèle sans autorisation écrite;
- signalent immédiatement tout incident ou toute utilisation non conforme;
- collaborent aux vérifications, aux enquêtes et aux mesures correctives;
- cessent l'utilisation d'un outil ou d'un renseignement dès que le Conseil l'exige.

5.3. Utilisation pédagogique par les élèves

5.3.1. Autorisation et encadrement

L'utilisation de l'intelligence artificielle par les élèves doit être autorisée et encadrée par un membre du personnel.

Avant l'activité, le membre du personnel précise :

- L'objectif pédagogique;
- l'outil autorisé;
- les fonctions permises;
- les renseignements qui peuvent ou ne peuvent pas être saisis;
- le niveau d'aide permis;
- les attentes relatives à l'attribution et à la remise du travail;
- les critères d'évaluation applicables;

- les conséquences possibles d'un usage non autorisé.

5.3.2. Conditions d'âge et comptes d'élèves

Les conditions d'âge et de consentement du fournisseur ainsi que les exigences du Conseil doivent être respectées.

La création d'un compte d'élève sur un service externe doit être autorisée selon le processus établi par le Conseil.

Un membre du personnel ne doit pas demander à un élève :

- De créer un compte personnel sur une plateforme non autorisée;
- d'utiliser une fausse date de naissance;
- de contourner les conditions d'âge ou de consentement;
- de fournir des renseignements personnels qui ne sont pas nécessaires à l'activité;
- d'accepter des conditions d'utilisation au nom du Conseil.

5.3.3. Évaluation des apprentissages

Le membre du personnel détermine, selon l'intention pédagogique, le degré d'utilisation de l'intelligence artificielle qui est permis.

Les pratiques d'évaluation doivent permettre de vérifier les apprentissages réels de l'élève. Elles peuvent notamment comprendre :

- L'observation du processus;
- des échanges avec l'élève;
- des traces de réflexion;
- des versions successives du travail;
- une démonstration orale ou pratique;
- une tâche réalisée dans un contexte supervisé;
- une comparaison entre la production remise et les connaissances démontrées par l'élève.

L'absence de mention d'une utilisation autorisée ne doit pas automatiquement être assimilée à une inconduite. Les attentes doivent avoir été clairement communiquées et adaptées à l'âge et au niveau scolaire.

5.3.4. Intervention en cas d'usage non autorisé

Lorsqu'un usage non autorisé est soupçonné, le membre du personnel :

- Recueille les renseignements pertinents;
- rencontre l'élève afin de lui permettre d'expliquer sa démarche;
- examine les traces du processus et les apprentissages démontrés;
- consulte la direction d'école lorsque la situation l'exige;

- applique les mesures pédagogiques, administratives ou disciplinaires prévues par les encadrements en vigueur;
- privilégie une intervention éducative, proportionnelle et adaptée à l'âge de l'élève.

Un outil de détection de contenu généré par l'intelligence artificielle ne doit pas constituer, à lui seul, une preuve suffisante d'un usage non autorisé.

5.4. Protection des renseignements personnels et confidentiels

5.4.1. Nécessité et minimisation

Avant de saisir ou de téléverser un renseignement dans un outil d'intelligence artificielle, la personne utilisatrice doit déterminer :

- Si l'utilisation est nécessaire;
- si l'outil et l'usage sont autorisés;
- si le renseignement peut être supprimé, remplacé, anonymisé, dépersonnalisé ou agrégé;
- si la même finalité peut être atteinte au moyen de données fictives ou moins sensibles;
- si la personne est autorisée à utiliser le renseignement à cette fin.

Seuls les renseignements strictement nécessaires peuvent être traités.

5.4.2. Renseignements interdits dans les outils non autorisés

Il est interdit de saisir, téléverser, copier, résumer, enregistrer, transcrire, analyser ou communiquer dans un outil non autorisé :

- Des renseignements personnels;
- des renseignements scolaires;
- des renseignements médicaux;
- des renseignements disciplinaires;
- des renseignements relatifs à l'emploi ou au rendement;
- des renseignements financiers;
- des renseignements protégés par le secret professionnel ou une obligation de confidentialité;
- des documents de réunion à huis clos;
- des identifiants, mots de passe ou renseignements de sécurité;
- des données institutionnelles non publiques;
- tout renseignement dont la divulgation pourrait porter préjudice à une personne ou au Conseil.

5.4.3. Outils autorisés

Dans un outil autorisé, le traitement de renseignements personnels ou confidentiels est permis uniquement lorsque :

- L'usage précis a été autorisé;
- la personne utilisatrice y est expressément habilitée;
- les renseignements sont nécessaires à la finalité autorisée;
- les mesures de sécurité prescrites sont appliquées;
- les conditions de conservation, d'accès et de suppression sont respectées;
- les résultats générés sont accessibles uniquement aux personnes autorisées.

5.4.4. Enregistrement, transcription et résumé de rencontres

L'intelligence artificielle ne doit pas être utilisée pour enregistrer, transcrire, résumer ou analyser une rencontre ou une conversation comportant des renseignements personnels ou confidentiels sans autorisation institutionnelle préalable.

Lorsque l'utilisation est autorisée :

- Les personnes concernées reçoivent un avis approprié;
- la finalité est clairement expliquée;
- l'accès au contenu est limité;
- la conservation respecte les règles de gestion documentaire;
- le contenu généré est vérifié avant d'être utilisé comme compte rendu ou pièce officielle.

5.5. Signalement et gestion des incidents

5.5.1. Obligation de signaler

Toute personne qui constate, soupçonne ou croit raisonnablement qu'un incident lié à l'intelligence artificielle est survenu doit le signaler sans délai à sa direction ou à sa superviseuse ou son superviseur immédiat ainsi qu'au Service informatique.

Le signalement est requis même lorsque :

- L'incident semble mineur;
- aucun préjudice n'a encore été constaté;
- l'outil a été fermé ou le contenu supprimé;
- la personne ignore si un renseignement a été conservé ou communiqué;
- l'incident résulte d'une erreur involontaire.

Le signalement rapide permet de limiter les effets de l'incident et constitue un facteur pris en considération dans l'évaluation de la situation.

5.5.2. Moyen de signalement

Le signalement est effectué par le mécanisme de soutien informatique établi par le Conseil ou, lorsqu'une intervention immédiate est requise, directement auprès du Service informatique et de la direction ou de la superviseure ou du superviseur immédiat.

5.5.3. Mesures immédiates

Lorsqu'un incident est constaté, la personne :

- Cesse l'utilisation de l'outil ou de la fonction concernée;
- ne supprime pas les preuves, les messages ou les fichiers pertinents, sauf instruction contraire;
- ne tente pas de corriger seule une situation pouvant compromettre les systèmes ou les données;
- suit les directives du Service informatique;
- transmet les renseignements factuels nécessaires à l'analyse;
- maintient la confidentialité de la situation.

5.5.4. Prise en charge

Le Service informatique coordonne la prise en charge technique de l'incident et collabore avec les responsables concernés afin de :

- Contenir l'incident;
- protéger les systèmes, les comptes et les renseignements;
- déterminer la nature, la portée et les conséquences possibles;
- identifier les personnes, les données et les systèmes touchés;
- préserver les éléments nécessaires à l'analyse;
- déterminer les mesures correctives et préventives;
- documenter les faits et les interventions;
- effectuer les communications et les signalements requis.

Lorsqu'un incident concerne des renseignements personnels, la personne responsable de l'accès à l'information et de la protection de la vie privée participe à son évaluation et détermine les suivis requis.

Lorsqu'un incident concerne un élève, la direction d'école et les services concernés déterminent les mesures adaptées à son âge, à ses besoins, à sa sécurité et à son bien-être.

Toute communication externe relative à un incident est coordonnée par le Service des communications et de l'imputabilité.

5.5.5. Documentation et suivi

Tout incident doit être documenté de manière proportionnelle à sa nature et à sa gravité.

La documentation peut notamment comprendre :

- La date et l'heure du signalement;
- une description factuelle de la situation;
- l'outil et la fonction concernés;
- les renseignements ou les personnes touchés;
- les mesures immédiates prises;
- les décisions et les communications effectuées;
- les mesures correctives et préventives;
- les recommandations découlant de l'analyse.

Les documents sont conservés conformément aux règles de gestion documentaire et d'accès applicables.

5.5.6. Analyse après l'incident

Lorsque la nature ou la gravité de l'incident le justifie, une analyse est réalisée afin de déterminer :

- Les causes de l'incident;
- l'efficacité des mesures de contrôle;
- les correctifs techniques, administratifs ou pédagogiques requis;
- les besoins de formation ou d'accompagnement;
- la nécessité de suspendre ou de retirer un outil;
- les modifications à apporter aux processus ou aux encadrements.

5.6. Non-conformité et mesures correctives

Toute utilisation non conforme peut entraîner la suspension ou le retrait de l'accès à l'outil, l'interruption de l'activité, la suppression sécuritaire des données ou toute autre mesure nécessaire pour protéger les personnes, les renseignements et les systèmes.

Selon la nature, la fréquence, l'intention et la gravité de la situation, le Conseil peut imposer :

- Un rappel des attentes;
- de la sensibilisation ou de la formation;
- un accompagnement ciblé;
- une révision des accès ou des autorisations;
- des mesures administratives;
- des mesures disciplinaires;
- des mesures prévues dans un contrat ou une entente;
- toute autre mesure conforme aux lois, aux conventions collectives, aux conditions de travail et aux directives administratives applicables.

5.7. Formation, sensibilisation et amélioration continue

Le CSCDGR offre de la formation et de l'accompagnement adaptés aux rôles et aux responsabilités des personnes utilisatrices.

La formation porte notamment sur :

- Les usages autorisés et interdits;
- la protection des renseignements personnels;
- la cybersécurité;
- les biais et les limites des outils;
- la vérification des résultats;
- les droits d'auteur et l'intégrité;
- le signalement des incidents;
- les attentes pédagogiques applicables aux élèves;
- la mission catholique de langue française.

Le Conseil recueille et analyse périodiquement des renseignements permettant d'évaluer la mise en œuvre de la présente directive.

Le suivi peut notamment porter sur :

- L'utilisation des outils autorisés;
- les demandes d'évaluation;
- les incidents et les risques observés;
- les besoins de formation;
- les résultats des projets pilotes;
- l'efficacité des mesures de protection;
- les modifications législatives, réglementaires, technologiques ou ministérielles.

6. RÉFÉRENCES ET FONDEMENTS LÉGISLATIFS

- [Directive sur l'utilisation responsable de l'intelligence artificielle | ontario.ca](#)
- [Le Centre Franco – Cadre pour l'utilisation de l'intelligence artificielle dans les conseils scolaires francophones de l'Ontario](#)
- Loi sur l'éducation, L.R.O. 1990, chap. E.2.
- Loi sur l'accès à l'information municipale et la protection de la vie privée, L.R.O. 1990, chap. M.56.
- Code des droits de la personne, L.R.O. 1990, chap. H.19.
- Loi de 2005 sur l'accessibilité pour les personnes handicapées de l'Ontario, L.O. 2005, chap. 11.
- Loi de 2000 sur la signature électronique, L.O. 2000, chap. 17.

- Loi de 2024 visant à renforcer la sécurité et la confiance en matière de numérique, L.O. 2024, chap. 16, annexe 1, ainsi que ses règlements d'application, lorsqu'ils s'appliquent aux conseils scolaires.
- Loi sur le droit d'auteur, L.R.C. 1985, chap. C-42.
- Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, chap. 5, lorsqu'elle s'applique.
- Règlement de l'Ontario 191/11, Normes d'accessibilité intégrées, pris en application de la Loi de 2005 sur l'accessibilité pour les personnes handicapées de l'Ontario.
- Règlement de l'Ontario 472/07, Comportement, mesures disciplinaires et sécurité des élèves, pris en application de la Loi sur l'éducation.

7. DIRECTIVES ADMINISTRATIVES ASSOCIÉES

- ADM-08 : Accès à l'information et protection de la vie privée (en élaboration)
- ADM-09 : Gestion des dossiers
- [ELE-08 : Code de conduite, prévention de l'intimidation et intervention, discipline progressive et sécurité dans les écoles](#)
- TIC-01 : Utilisation des technologies
- TIC-03 : Cybersécurité et tests d'hameçonnage (en élaboration)
- PED-06 : Évaluation et communication du rendement de l'élève
- RH-08 : Mesures disciplinaires

8. ANNEXES

Sans objet.

9. FORMULAIRES

Sans objet.

10. CYCLE DE RÉVISION

La présente directive est révisée au minimum tous les cinq (5) ans ou plus fréquemment, au besoin.