Ontario

Ministère des Services au public et aux entreprises et de l’Approvisionnement
Stratégie, Intelligence artificielle, Données
Division de l’intelligence artificielle

Utilisation des technologies numériques en fonction de l’âge : Pratiques exemplaires pour les organismes publics de l’Ontario

Table des matières

Introduction

Ces pratiques exemplaires s'adressent aux organismes du secteur public de l'Ontario qui aident les enfants et les jeunes à utiliser les technologies numériques de façon sécuritaire. Elles s'ajoutent au nouveau Règl. de l'Ont. 52/26 en vertu de la Loi de 2024 visant à renforcer la sécurité et la confiance en matière de numérique. Cette loi fournit au gouvernement une base pour renforcer la **cybersécurité**, améliorer la **protection de la vie privée des enfants** et favoriser une utilisation responsable de l'**intelligence artificielle**. Les renseignements fournis dans le présent document ne doivent pas être considérés comme des directives officielles pour les secteurs et ils ne créent aucune obligation légale.

Ce document:

- donne un **aperçu des principaux enjeux et concepts** liés à la sécurité numérique;
- présente les **ressources** permettant d'évaluer les pratiques technologiques actuelles;
- recommande des **pratiques exemplaires particulières** afin d'éviter tout préjudice potentiel aux enfants et aux jeunes.

Ce document s'appuie sur quatre principes directeurs :

1) Donner la priorité à l'apprentissage de la sécurité numérique.
2) Protéger la vie privée et les données des enfants et des jeunes.
3) Utiliser des applications et des services sécurisés.
4) Utiliser l'intelligence artificielle (IA) de manière responsable.

Les recommandations et les renseignements fournis dans le présent document ne sont pas obligatoires. Certaines politiques officielles existantes sont mentionnées ci-dessous ; toutefois, il ne s'agit pas d'une liste exhaustive des politiques applicables en Ontario et au Canada.

Chaque organisme a pour responsabilité de vérifier qu'il comprend et respecte l'ensemble des lois, des règlements, des directives ou des politiques applicables en matière de vie privée et de protection des enfants et des jeunes utilisant les technologies numériques. En cas de conflit avec les recommandations du présent document, les lois, les règlements, les directives et les politiques applicables l'emporteront.

Voici quelques exemples de politiques existantes pouvant s'appliquer :

- *Loi de 2017 sur les services à l'enfance, à la jeunesse et à la famille*
- *Loi sur l'éducation*
- *Loi sur l'accès à l'information et la protection de la vie privée*
- *Loi sur l'accès à l'information municipale et la protection de la vie privée*

Public cible

Ce document s'adresse aux organismes tels que :

- les conseils scolaires;
- les sociétés d'aide à l'enfance et les organismes de bien-être des enfants et des familles autochtones

Néanmoins, ce document peut être utile à toute personne qui veut comprendre et adopter les pratiques exemplaires pour accompagner les enfants et les jeunes dans leur utilisation des technologies numériques.

Recommandations pour une utilisation des technologies appropriée en fonction de l'âge

1. Prioriser l'apprentissage de la sécurité numérique

La première étape pour protéger les enfants et les jeunes consiste à comprendre les risques liés au numérique auxquels ils sont exposés. Cela passe par l'éducation des personnes qui travaillent auprès d'eux, des parents et des tuteurs, ainsi que des enfants et des jeunes eux-mêmes.

Dans le présent document, le terme « droits » d'un enfant ou d'un adolescent désigne la garantie des droits humains et des libertés fondamentales dont jouissent les personnes âgées de moins de 18 ans, qui leur assure une protection contre la discrimination et les préjudices (Convention relative aux droits de l'enfant des Nations Unies).

Les organismes du secteur public doivent veiller à ce que leurs politiques numériques continuent de respecter les droits des enfants et des jeunes à mesure que les technologies évoluent. Ces politiques doivent pouvoir s'adapter et être régulièrement révisées et mises à jour en collaboration avec les enfants, les jeunes, les familles, les collectivités et les experts en la matière afin de conserver leur pertinence et leur efficacité.

Une technologie adaptée en fonction de l'âge

Les enfants et les jeunes devraient utiliser des technologies numériques adaptées à leur stade de développement, en adéquation avec leur maturité cognitive et conformes à leur intérêt supérieur.

Les décisions concernant les applications numériques utilisées par les enfants et les jeunes, y compris la manière dont ils les utilisent et les raisons pour lesquelles ils le font, devraient viser à servir leur intérêt supérieur, notamment leur santé et leur bien-être, leur liberté d'expression, leur sécurité et leur vie privée. Les enfants et les jeunes ont des besoins, des contextes, des capacités et des centres d'intérêt variés ; les décisions relatives à l'utilisation des technologies numériques devraient donc s'efforcer de refléter cette diversité et d'en tenir compte.

Les organismes qui fournissent des services publics aux enfants et aux jeunes devraient aider les parents ou tuteurs, les personnes qui s'occupent d'eux et les éducatrices et les éducateurs à comprendre comment la technologie peut influencer les étapes importantes du développement des enfants et comment protéger leurs droits (Child Rights by Design (en anglais seulement), Digital Futures Commission). Cela permet de promouvoir des approches différenciées, plus à même d'accompagner chaque enfant dans son développement.

La Société canadienne de pédiatrie Cette association recommande de limiter le temps que les enfants de plus de cinq ans passent devant un écran à moins de deux heures par jour (et à moins d'une heure pour les enfants âgés de deux à cinq ans).

Comprendre la sécurité numérique

Bien que la technologie offre des possibilités en matière d'apprentissage et de créativité, elle comporte également des risques importants. Les chercheurs s'accordent à dire qu'une utilisation excessive des outils numériques, tels que les réseaux sociaux et les jeux en ligne, peut avoir des répercussions négatives sur la santé et le bien-être des enfants et des jeunes. L'hypertrucage, le cyberharcèlement et d'autres expériences préjudiciables en ligne peuvent avoir d'énormes conséquences sur la santé mentale des enfants et des jeunes.

Risques communs

Les enfants et les jeunes sont exposés à certains risques communs lorsqu'ils sont en ligne, notamment :

- **Risques liés au contenu** : exposition à des contenus inappropriés, comme des images à caractère sexuel ou violent, certaines formes de publicité préjudiciable et des sites Web présentant des comportements dangereux.
- **Risque lié aux relations**: interaction inappropriée entre un enfant et un adulte. Cela peut notamment se traduire par le fait qu'un adulte sollicite des faveurs sexuelles auprès d'un enfant ou tente de l'influencer en lui inculquant des idéologies radicales ou extrémistes.
- **Risque lié au comportement** : comportements négatifs résultant de l'exposition à des contenus et à des relations nuisibles. Ces comportements ont des répercussions négatives tant sur l'enfant que sur ses pairs et peuvent inclure le harcèlement, l'automutilation ou la diffusion de contenus préjudiciables.
- **Risques liés aux contrats** : lorsqu'un enfant accepte un accord comportant des conditions pouvant relever de l'exploitation, sans disposer de moyens suffisants pour exercer un contrôle ou s'en soustraire. Cela peut notamment concerner l'acceptation des conditions d'utilisation ou des conditions générales d'un fournisseur commercial proposant un produit ou un service numérique.

Outre ces risques, les obstacles liés à l'accès au numérique chez les enfants et les jeunes peuvent nuire à leur littératie numérique. Cette littératie numérique insuffisante pourrait accroître leur vulnérabilité face aux dangers du numérique, tels que la manipulation psychologique en ligne.

Respecter les protocoles relatifs aux données autochtones

Les enfants et les jeunes des Premières Nations, des Inuits, des Métis et des communautés autochtones en milieu urbain ont des besoins uniques sur les plans physique, émotionnel, social, culturel, linguistique et spirituel. Ces besoins peuvent inclure des liens étroits avec leur famille proche et élargie, leur communauté et les autres. Pour déterminer l'intérêt supérieur et les droits des enfants et des jeunes autochtones, il est souvent nécessaire d'avoir une compréhension plus large des facteurs susceptibles de nuire à leur santé et à leur bien-être.

Il est recommandé aux communautés des Premières Nations, des Inuits et des Métis de s'occuper elles-mêmes de la gestion des données relatives à leurs communautés, à leurs terres, à leurs populations et à leurs ressources. Le respect des différentes attentes des Premières Nations, des Métis et des Inuits en matière de vie privée et des renseignements peut aider les enfants et les jeunes autochtones à utiliser les technologies numériques d'une manière qui favorise leur santé et leur bien-être tout en respectant les pratiques culturelles.

Mesures recommandées à envisager

- Promouvoir la littératie numérique afin d'aider les enfants et les jeunes à utiliser les technologies numériques de manière sécuritaire et responsable.
- Donner aux enfants et aux jeunes les moyens de s'exprimer librement sur leurs expériences numériques. Leur permettre de donner leur avis sur la manière dont ils utilisent les technologies numériques et de contribuer à l'élaboration des politiques en la matière.
- Sensibiliser les enfants, les jeunes et les parents ou tuteurs aux risques liés aux technologies et au cyberharcèlement (conformément à la *Loi sur l'éducation* dans le cadre de la note Politique/Programmes no 144 — prévention et intervention en matière d'intimidation).
- Se renseigner sur les protocoles de gestion des données autochtones fondés sur les distinctions. Collaborer avec les organismes autochtones chaque fois que cela est possible afin de veiller à ce que la technologie utilisée en milieu scolaire ne porte pas atteinte aux principes relatifs aux données, aux traités ou à d'autres valeurs culturelles importantes.

Ressources utiles

- Pour en savoir plus sur **la prise de décisions concernant l'utilisation des technologies numériques par les enfants**, consultez l'outil d'évaluation des répercussions sur les droits de l'enfant (ERDE) du gouvernement du Canada.
  - Les guides pédagogiques du Commissaire à l'information et à la protection de la vie privée de l'Ontario pour aider les enfants et les jeunes à comprendre l'importance de la protection de la vie privée.
  - Les renseignements, les outils et les autres ressources du Commissariat à la protection de la vie privée du Canada pour aider les adultes qui travaillent dans le secteur public à aborder la question de la protection de la vie privée avec les enfants et les jeunes.
- Pour en savoir plus sur les **protocoles de données autochtones fondés sur les distinctions**, veuillez consulter :
  - les principes de PCAP® des Premières Nations (propriété, contrôle, accès, possession).
  - les principes de PCAI des Métis (propriété, contrôle, accès et intendance).
  - les principes des Inuits Qaujimajatuqangit (savoir traditionnel).
- Pour en savoir plus sur le temps d'écran recommandé, consultez le site de la Société canadienne de pédiatrie.
- Pour en savoir plus sur la cybersécurité dans le secteur public, consultez les ressources proposées par le Centre d'excellence pour la cybersécurité.

2. Protéger les données et la vie privée des enfants et des jeunes

Les risques liés à la vie privée augmentent à mesure que les enfants et les jeunes utilisent de plus en plus les technologies numériques, en particulier lorsqu'ils doivent fournir des renseignements personnels.

Par exemple, le fait de partager des renseignements comme le lieu où se trouve un enfant pourrait permettre aux autres de le trouver et de s'en prendre à lui. Cela est particulièrement préoccupant pour les enfants et les jeunes pris en charge, qui sont souvent la cible de la traite des personnes ou qui peuvent être séparés de leur famille pour leur propre sécurité.

Il est recommandé d'adopter une approche équilibrée afin de tirer parti des avantages que les technologies offrent aux enfants, aux jeunes, aux éducatrices et éducateurs, aux parents ou tuteurs et aux personnes qui s'occupent d'eux, tout en réduisant les risques liés à la vie privée et les conséquences nuisibles.

Principe de minimisation des données

La « minimisation des données » est le principe qui consiste à limiter la collecte, le traitement, le stockage et le partage des données ou renseignements personnels au strict nécessaire pour fournir un service particulier.

Il est recommandé de vérifier dans quelle mesure les produits ou outils ont accès aux données personnelles des enfants et des jeunes. Limiter l'accès à ces données réduit le risque qu'elles soient utilisées à des fins préjudiciables, par exemple dans le cadre de pratiques de marketing prédateur, de profilage ou de monétisation des données.

En ce qui concerne les sociétés d'aide à l'enfance, le principe de minimisation des données est énoncé dans la *Loi de 2017 sur les services à l'enfance, à la jeunesse et à la famille, partie X*.

Faire preuve de transparence quant à la manière dont les données sont collectées, utilisées et partagées

Expliquez clairement aux enfants et aux jeunes, ainsi qu'à leurs parents, à leurs tuteurs et aux autres personnes qui s'occupent d'eux, ce à quoi ils peuvent s'attendre en ce qui concerne leurs données et renseignements personnels lorsqu'ils utilisent les technologies numériques. Il est recommandé que les enfants, les jeunes et leurs parents ou tuteurs soient informés de la manière dont leurs données sont utilisées ou traitées et puissent contrôler les renseignements qui sont partagés.

Il est également considéré comme une pratique exemplaire d'informer une personne et, le cas échéant, de lui demander son accord ou son consentement quant à l'utilisation de ses données. Le consentement éclairé signifie qu'une personne comprend clairement comment ses données seront utilisées et y consent volontairement. Voici quelques éléments importants permettant de veiller au consentement éclairé :

- l'objectif de la technologie ou de l'application utilisée;
- les renseignements qui sont collectés;
- la manière dont leurs renseignements seront utilisés;
- les risques liés au partage de leurs renseignements.

Mesures recommandées à envisager

- Fournir aux enfants et aux jeunes des outils et des ressources pour les aider à comprendre leurs droits à la vie privée et leur donner les moyens de les faire valoir. Appliquer les paramètres de confidentialité et de sécurité les plus stricts possibles aux applications et aux outils numériques utilisés par les enfants et les jeunes dans les établissements publics dans le but de protéger leurs renseignements personnels. Ces paramètres devraient être définis par défaut.
    - Désactiver le suivi de géolocalisation par défaut. Lorsque la géolocalisation est nécessaire, veiller à ce que le logiciel indique clairement quand la position de l'utilisateur est suivie.
    - Utiliser si possible des comptes anonymisés ou génériques.
    - Évaluer les risques liés à l'utilisation d'appareils connectés avant de les confier à des enfants et à des adolescents. Surveiller les appareils connectés pour s'assurer que le Wi-Fi, le Bluetooth, les caméras et les microphones sont désactivés lorsqu'ils ne sont pas utilisés.
- Si vous envisagez d'utiliser un outil ou une application numérique, il est important d'examiner comment les données sont utilisées dans ces applications et d'évaluer s'il existe des risques. Réaliser une Évaluation de l'impact sur la protection de la vie privée (EIPVP) dans les situations suivantes :
    - Lors de la mise en œuvre d'un nouveau système qui collecte, utilise ou communique des renseignements personnels.

    - Lors de la modification d'un système existant qui collecte, utilise ou communique des renseignements personnels.
    - Consulter l'EIPVP afin de surveiller et d'examiner régulièrement l'utilisation des données dans le système.
- Veiller à ce que les applications expliquent, dans un langage clair, comment les renseignements sont recueillis. Dans la mesure du possible, traduire les avis dans les langues utilisées par les collectivités des enfants.
- Dans la mesure du possible, publier les conditions d'utilisation ou les contrats de licence d'utilisation des applications afin de favoriser la transparence quant à l'utilisation des renseignements personnels.
- Établir des procédures pour aviser les parents ou tuteurs et les personnes qui s'occupent de l'enfant lorsque vous avez connaissance d'incidents ou de préjudices, comme le cyberharcèlement ou l'hypertrucage.
- Inclure dans les contrats conclus avec des fournisseurs tiers des dispositions visant à garantir la protection de la vie privée des enfants et des jeunes ainsi que la minimisation des données dans les applications ou les services, lesquelles peuvent s'ajouter aux dispositions prévues par la loi. Par exemple :
    - permettre aux élèves d'accéder à leurs renseignements personnels et de les rectifier;
    - s'engager à ne collecter des données qu'aux fins décrites dans l'accord;
    - inclure des outils de confidentialité facilement accessibles, comme « voir toutes mes données », « télécharger mes données », « supprimer toutes mes données », etc.

Ressources utiles

- Pour en savoir plus sur **la manière de protéger la vie privée des élèves** lors de l'utilisation des technologies numériques, veuillez consulter La Charte de la protection de la vie privée numérique pour les écoles ontariennes du Commissaire à l'information et à la protection de la vie privée.
- Pour en savoir plus sur **la manière d'assurer la transparence concernant les technologies** utilisées dans les écoles, veuillez consulter le Guide des exigences en matière de notification et de consentement pour l'utilisation d'outils numériques de l'Ontario Association of School Business Officials (OASBO).

3. Utiliser des applications et des services sécurisés

Les produits numériques sont de plus en plus conçus pour influencer subtilement le comportement des utilisateurs. Les pratiques de conception visant à renforcer l'engagement peuvent avoir des répercussions négatives sur les utilisateurs, en particulier les enfants et les jeunes. Sensibiliser les parents ou tuteurs, les enfants et les jeunes, ainsi que les personnes qui s'occupent d'eux, à des pratiques numériques plus sécuritaires peut aider à favoriser des choix plus éclairés et à réduire les risques.

Modèles de conception à des fins de manipulation

Les modèles de conception à des fins de manipulation utilisés dans le domaine technologique incitent délibérément les utilisateurs à accomplir des actions qu'ils n'auraient pas effectuées autrement, par exemple :

- s'inscrire aux notifications par courriel;
- effectuer un achat;
- rester en ligne plus longtemps que prévu.

Parmi les exemples de ces modèles à surveiller, on peut citer les stratégies d'incitation douce, les fils d'actualité addictifs et le marketing prédateur.

L'incitation douce est une caractéristique d'application ou de conception logicielle qui encourage les utilisateurs à faire des choix qui les mènent dans la direction souhaitée par le concepteur ou le développeur.

La stratégie d'incitation douce peut être utilisée de manière positive ou négative :

- une incitation douce de type neutre offre aux utilisateurs un choix impartial;
- une incitation douce de type positif peut inciter les utilisateurs à demander de l'aide en cas de besoin;
- une incitation douce de type négatif peut proposer plusieurs choix aux utilisateurs, tout en favorisant l'un d'entre eux.

Les stratégies d'incitation douce peuvent encourager les enfants et les jeunes à désactiver les fonctionnalités de protection de la vie privée dans l'application. Les applications utilisées par les enfants et les jeunes ne devraient pas utiliser de stratégies d'incitation douce visant à réduire la protection de la vie privée.

Voir l'annexe A pour quelques exemples de types de stratégies d'incitation douce.

Les fils d'actualité addictifs sont fréquents sur les réseaux sociaux et les applications numériques, y compris celles qui utilisent l'IA. Ils sont conçus pour maintenir l'intérêt des utilisateurs en leur proposant du contenu pendant de longues périodes. Ces fils d'actualité contribuent souvent à une utilisation excessive.

Les fils d'actualité addictifs peuvent utiliser :

- **des algorithmes personnalisés** : pour afficher du contenu adapté à des utilisateurs particuliers afin de maintenir leur intérêt.
- **le défilement infini** : le contenu n'a pas de « fin », ce qui incite à continuer d'utiliser l'application.
- **la nouveauté constante** : des notifications et la diffusion continue de nouveaux contenus pour inciter les utilisateurs à revenir sur l'application.

Voir l'annexe B pour de plus amples renseignements sur les fils d'actualité addictifs.

Le marketing prédateur peut cibler les enfants et les jeunes et leur proposer des publicités qui peuvent nuire à leur santé (par exemple, des collations très sucrées) ou à leur bien-être (par exemple, des jeux gratuits addictifs comportant des microtransactions).

Voir l'annexe C pour de plus amples renseignements sur le marketing prédateur.

Mesures recommandées à envisager

- Veiller à ce que les applications numériques utilisées par les enfants et les jeunes dans les établissements publics ne contiennent aucune publicité.
- Se méfier et éviter les technologies qui emploient des modèles de conception visant à manipuler les utilisateurs.
- S'informer sur les effets nuisibles des fils d'actualité addictifs sur la santé.
- Limiter le marketing prédateur en utilisant des comptes anonymes contenant le moins de renseignements personnels possible.

4. Utiliser l'intelligence artificielle (IA) de manière responsable

L'intelligence artificielle (IA) est de plus en plus utilisée par les enfants et les jeunes, ainsi que par les organismes qui les accompagnent. Dans les services publics, l'IA peut faciliter l'apprentissage, réduire le temps consacré aux tâches routinières et améliorer le bon fonctionnement des programmes. En expliquant aux enfants et aux jeunes comment fonctionne l'IA, on peut les aider à l'utiliser de manière sécuritaire et responsable.

L'IA générative (IAG) est de plus en plus utilisée pour traiter des données, produire des textes et générer des contenus multimédias, comme des images, des vidéos ou des fichiers audio.

Voici quelques outils d'IA générative couramment utilisés :

- ChatGPT
- Microsoft Copilot
- Google Gemini
- Midjourney
- Claude
- DALL-E

Comme l'IA est une technologie nouvelle qui évolue rapidement, il est important de se tenir informé des risques particuliers qui y sont associés :

L’IA peut renforcer les préjugés

Il faut sensibiliser les enfants et les jeunes au fait que l’IA peut parfois être biaisée. Comme l’IA apprend à partir de vastes ensembles de données pouvant refléter des préjugés humains, elle peut involontairement renforcer les stéréotypes. Par exemple :

- Les outils d’IA peuvent être injustes envers les groupes marginalisés si les données sur lesquelles ils ont été entraînés sont incomplètes ou déséquilibrées.
- L’IA peut reproduire ou renforcer des préjugés raciaux ou culturels, ce qui peut conduire à des résultats injustes.

L’utilisation de l’IA n’est pas toujours transparente

Lorsque les jeunes utilisent des outils d’IA, ils doivent bien comprendre comment cette technologie fonctionne et comment leurs renseignements sont utilisés. La transparence contribue à protéger leurs renseignements, les aide à comprendre quelles données sont collectées et leur permet de reconnaître les situations qui ne semblent pas sécuritaires.

Il convient de bien comprendre les limites et les risques liés à la transparence en matière d’IA, par exemple :

- Certains outils d’IA peuvent stocker les renseignements personnels qui leur sont communiqués, ou utiliser des données et du contenu original pour entraîner des modèles sans consentement explicite.
- Les modèles d’IA n’expliquent souvent pas comment leurs résultats sont générés, ce qui les rend moins transparents.

L’IA peut générer de la mésinformation et de la désinformation

L’IA peut générer des contenus trompeurs ou totalement faux. Cela peut être préjudiciable pour les enfants et les jeunes, mais cela peut aussi être le moment idéal pour leur enseigner la littératie numérique.

Les contenus faux et nuisibles comprennent :

- **La mésinformation** : toute information fausse, inexacte ou subjective présentée comme un fait.
- **La désinformation** : des informations intentionnellement fausses visant à induire en erreur ou à manipuler (par exemple, les canulars et la propagande).
- **L’hypertrucage** : des images, des vidéos ou des enregistrements audio très réalistes, mais faux, susceptibles de semer la confusion ou de nuire à la réputation d’une personne.

Mesures recommandées à envisager

- Établir des règles claires avec les enfants et les jeunes sur l’utilisation de l’IA en toute sécurité, notamment en ce qui concerne les risques liés à son utilisation, les situations dans lesquelles il ne faut pas utiliser les outils d’IA, et la manière dont ils peuvent protéger leurs renseignements personnels et leur vie privée lorsqu’ils utilisent l’IA.
- Élaborer des politiques claires relatives à l’utilisation de l’IA qui tiennent compte des risques juridiques, éthiques et liés à la protection de la vie privée. Examiner ces politiques avec les enfants, les jeunes, les parents, les éducatrices, les éducateurs et la collectivité afin de s’assurer que l’utilisation de l’IA ne porte pas préjudice aux enfants ou aux jeunes.
- Renforcer la littératie des enfants et des jeunes en matière d’IA ainsi que leur esprit critique, afin qu’ils puissent déterminer si les contenus générés par l’IA sont exacts et fiables.
- Mettre en œuvre un processus de gestion des risques liés à l’IA lorsque les enfants et les jeunes ont accès à des outils d’IA.
- Utiliser, dans la mesure du possible, des outils d’IA déjà approuvés afin de s’assurer qu’ils respectent les normes minimales en matière de sécurité et de qualité.

Ressources utiles

- Pour mieux comprendre les lignes directrices pour les ministères et les organismes provinciaux concernant l'utilisation transparente, responsable et justifiée de l'IA, veuillez consulter la Directive sur l'utilisation responsable de l'intelligence artificielle de l'Ontario (qui fait partie du Cadre ontarien pour la fiabilité de l'intelligence artificielle).
    - Cette directive s'applique uniquement aux ministères et aux organismes provinciaux, mais peut constituer une ressource utile pour obtenir des renseignements sur l'utilisation responsable de l'IA.

Conclusion

La technologie évolue sans cesse, et nous sommes conscients que ces recommandations doivent elles aussi évoluer en permanence. Il s'agit d'un document évolutif qui sera régulièrement révisé et mis à jour.

Le ministère aimerait connaître votre avis sur ce document. Si vous avez des questions ou des commentaires à ce sujet, veuillez nous envoyer un courriel à l'adresse Digital.Government@ontario.ca.

Remerciements

Vous trouverez ci-dessous la liste des ministères et des secteurs d'activité qui ont examiné le présent document et fait part de leurs commentaires à ce jour :

Ministère	**Division**
Ministère des Services à l'enfance et des Services sociaux et communautaires	Division du bien-être et de la protection de l'enfance Division des politiques stratégiques
Ministère de l'Éducation	Division des politiques stratégiques et de la planification
Ministère des Affaires autochtones et de la Réconciliation économique avec les Premières Nations	Division des politiques stratégiques et de la planification
Ministère des Services au public et aux entreprises et de l'Approvisionnement	Division des Archives publiques et de la protection de la vie privée Division de l'intelligence artificielle TechGouvON Direction des services juridiques

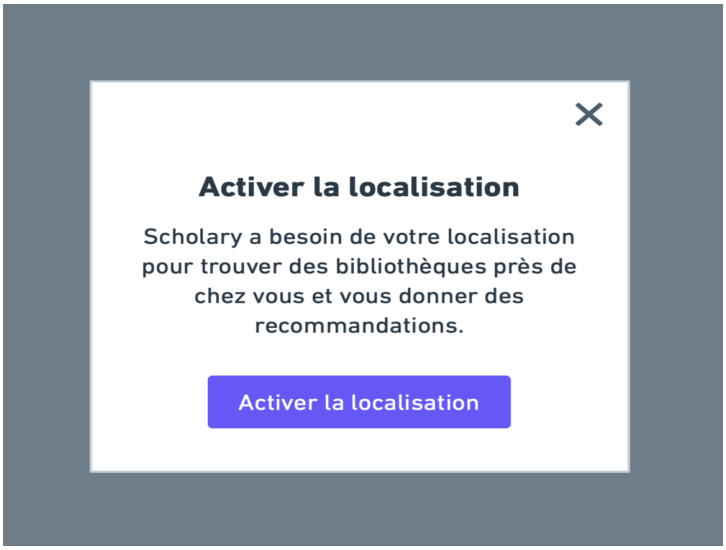
Annexe A : Exemples de stratégies d’incitation douce

Le tableau ci-dessous présente trois exemples différents de types d’incitation douce pour un scénario donné : une application demandant l’accès à la localisation.

Exemples de stratégies d’incitation douce de type négatif, neutre et positif pour les demandes d’accès à la localisation

Incitation douce de type négatif

- Le fait qu’il n’y ait qu’un seul bouton donne l’impression que l’activation est la seule option possible.
- Il n’est pas clair que les utilisateurs peuvent ignorer la demande en cliquant sur l’icône « x ».
- La formulation laisse entendre que l’accès à la localisation est nécessaire au bon fonctionnement de l’application.



Incitation douce de type neutre

- Explique en quoi consiste l’activation de la localisation et précise clairement qu’elle n’est pas obligatoire.
- Propose deux options équivalentes : activer la localisation ou passer cette étape et décider plus tard.

Incitation douce de type positif

- Explique en quoi consiste l’activation de la localisation et précise clairement qu’elle n’est pas obligatoire.
- Incite (encourage) les jeunes utilisateurs à demander l’aide d’un adulte avant de faire leur choix.

Annexe B : Modèles de fils d’actualité addictifs

Les fils d’actualité addictifs sont utilisés par diverses applications de réseaux sociaux pour maximiser l’engagement des enfants et des jeunes. Ces applications emploient différents modèles pour inciter les enfants et les jeunes à revenir régulièrement les utiliser. Voici quelques exemples de ces stratégies :

Contenu personnalisé : les applications collectent des données sur les centres d’intérêt, l’humeur et les habitudes des utilisateurs afin de personnaliser le contenu proposé aux enfants et aux jeunes. Ces données sont intégrées à un algorithme qui détermine ce que l’utilisateur voit en fonction de ces tendances, ce qui l’incite à rester plus longtemps sur l’application.

Gratification instantanée : En raison de leur facilité d’accès et de la rapidité avec laquelle elles procurent une récompense, les applications de réseaux sociaux fournissent instantanément de la dopamine aux enfants et aux jeunes. Des actions courantes, comme aimer, commenter et recevoir des notifications provoquent de petites poussées de dopamine, ce qui incite les utilisateurs à revenir pour en obtenir davantage.

Liens sociaux artificiels : Le sentiment qu’un enfant est socialement attaché à une communauté. Le cerveau libère de la dopamine lorsque les individus tissent des liens humains, ce qui les incite à renouveler cette expérience (Addictive potential of social media, explained, Stanford Medicine (en anglais seulement). Ce sentiment d’appartenance à une communauté pousse les utilisateurs à rester actifs sur les réseaux sociaux pour ne pas passer à côté d’interactions sociales ou d’actualités communautaires.

Annexe C : Exemples de marketing prédateur

Le marketing prédateur consiste, pour une application tierce, à utiliser des renseignements afin d’identifier les centres d’intérêt d’un enfant ou d’un jeune, puis à lui proposer des publicités ciblées en fonction de ces centres d’intérêt. Ces pratiques impliquent tromperie, coercition et manipulation afin d’exploiter les vulnérabilités des jeunes.

Voici quelques exemples de marketing prédateur :

- **Collecte de données** : recueillir des renseignements sur les centres d’intérêt d’un enfant ou d’un adolescent et diffuser des publicités en fonction de ces centres d’intérêt.
- **Manipulation sur les réseaux sociaux** : demander à des influenceurs de promouvoir un produit en l’intégrant parfaitement à leur contenu, de sorte qu’il devient difficile de distinguer ce qui relève de la publicité de ce qui relève du contenu.
- **Ludification** : utiliser les principes du jeu (comme la compétition avec les autres, l’attribution de points et de badges) pour encourager et motiver les enfants et les jeunes à interagir avec l’application, notamment en les incitant à effectuer des achats dans l’application pour obtenir des avantages supplémentaires.
- **Marketing fondé sur le pouvoir de persuasion des enfants** : inciter les enfants et les jeunes à demander sans cesse à leurs parents ou tuteurs d’acheter un produit ou un service.