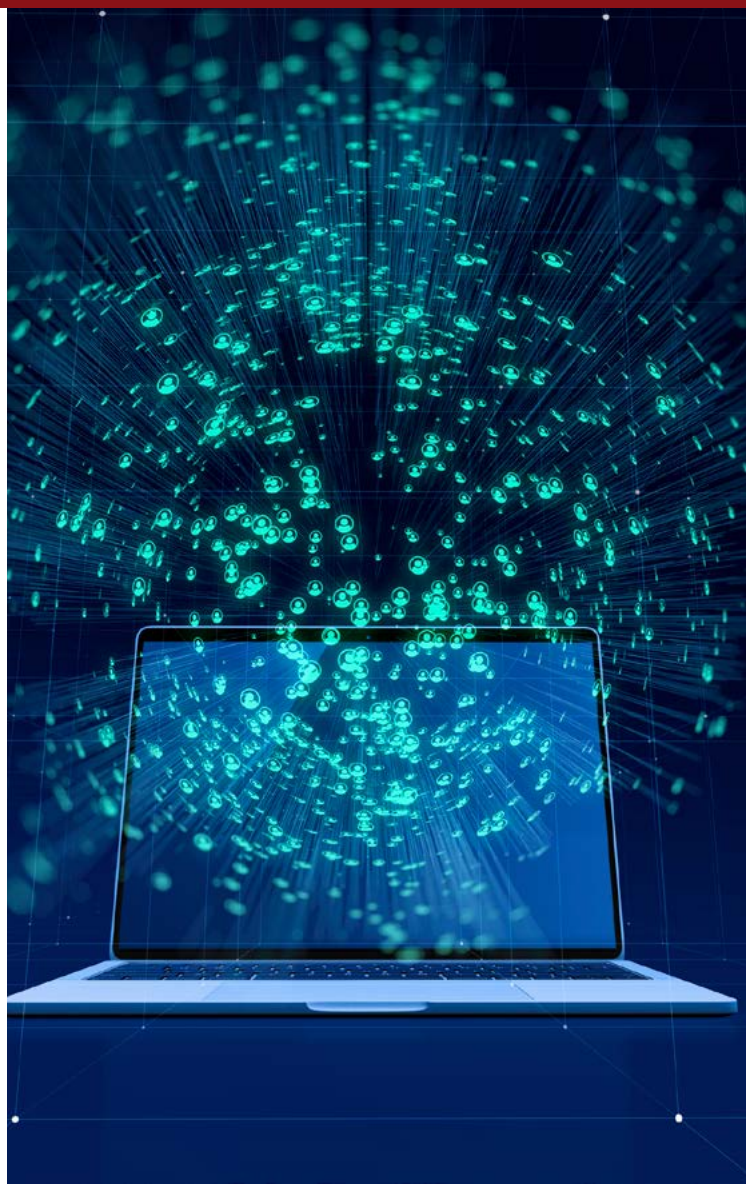
AI Bytes

Making Sense of Artificial Intelligence in Literacy and Basic Skills Education

A Contact North | Contact Nord and Literacy Link South Central publication

e-Channel
Apprentissage en ligne

Literacy Link South Central



Welcome to *AI Bytes*, your digital digest for the latest in artificial intelligence (AI) information for literacy and basic skills (LBS).

The integration of AI in adult education raises fundamental questions about the nature of learning, equity, and trust. For learners who navigated prior educational barriers and societal pressures, the promise of personalized pathways must be tempered with critical ethical considerations:

- How do we ensure AI algorithms reflect diverse perspectives and promote genuine learner agency?
- How can we mitigate the risk of algorithmic bias and the subtle erosion of human connection in learning environments?

In the context of LBS programs, where trust is crucial, this edition explores the ethical dimensions of AI implementation. It analyzes current legislative frameworks, evaluates strategies for fostering critical thinking, and proposes principles for equitable, transparent, and ethical AI-driven education.

Inside *AI Bytes*

This edition is the last of a series of six scheduled for distribution throughout 2024 and 2025. We specifically designed it to provide valuable insights and resources for educators in adult education, with an emphasis on LBS programs.

In this edition, we cover:

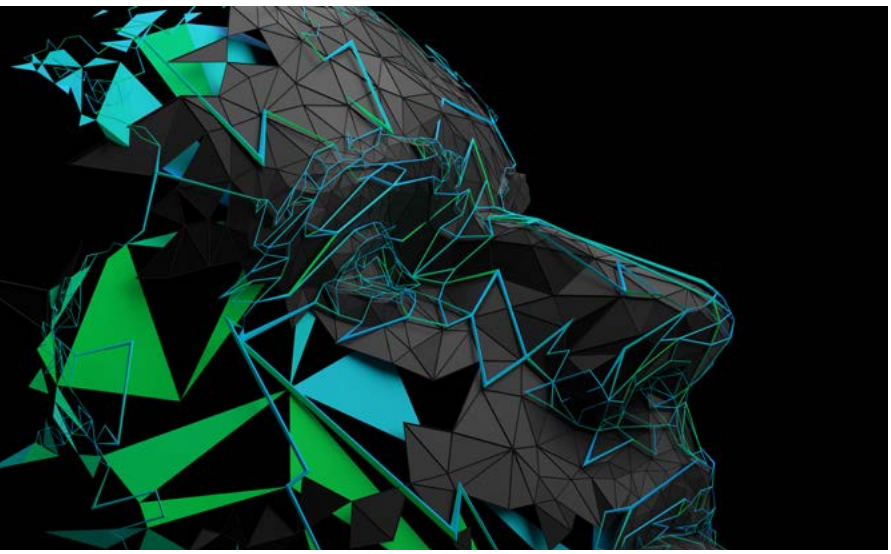
- Overview of AI Legislation in Canada
- The Canadian AI Regulatory Landscape tailored for LBS
- Six Actionable Steps for Adult Educators
- 10 Actionable Steps for Organizations

Meet the *AI Bytes* team

Carolina Cohoon is an EdTech Consultant at Literacy Link South Central. Her professional background encompasses education and rehabilitation, with a passion for inclusion and accessibility. Carolina is dedicated to designing learning experiences that celebrate and embrace diversity. Her interest in artificial intelligence (AI) is fueled by her enthusiasm for innovation, knowledge sharing, enhancing accessibility, and improving the learning experience through personalized learning adaptations that AI can offer within the framework of Universal Design for Learning (UDL).

Jeremy Marks works for Literacy Link South Central as a project manager and edtech researcher. He completed the Teacher/Trainer of Adults program at Conestoga College and now teaches essential skills in London. Jeremy has taught learners in public and secondary schools, colleges, and universities in Canada and the U.S. since 2002. His fascination with AI comes from his longstanding passion for educational theory and cognitive philosophy.

* This bulletin is edited by Contact North | Contact Nord.



Overview of AI Legislation in Canada

Federal Legislation

Bill C-27

Bill C-27, also known as the Digital Charter Implementation Act, 2022, is a pending piece of legislation that introduces three significant laws:

1. ***Consumer Privacy Protection Act* (CPPA):** This Act focuses on enhancing personal data protection and ensuring transparency in how personal information is handled by organizations. It includes measures such as data mobility rights and the right to request the disposal of personal information. Consumer Privacy Protection Act
2. ***Personal Information and Data Protection Tribunal Act*:** This Act establishes a tribunal to handle appeals and impose penalties related to violations of privacy regulations, acting on the recommendations of the Privacy Officer. C-27 (44-1) - LEGISinfo - Parliament of Canada
3. ***Artificial Intelligence and Data Act* (AIDA):** This Act focuses on high-impact AI systems, requiring developers to meet safety, fairness, and accountability standards. It will be enforced by the Minister of Innovation, Science and Economic Development (ISED) and supported by an Artificial Intelligence and Data Commissioner. AI regulation in Canada: New laws and regulations to know | Canadian Lawyer

Aside from the pending Bill C-27, a **Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems** was released by the federal

government. This Code outlines measures for organizations developing or managing advanced generative AI systems, such as ChatGPT, to ensure responsible and ethical practices.

It outlines principles such as accountability, safety, fairness, and transparency for organizations developing or managing generative AI technologies. Canadian Artificial Intelligence Safety Institute

Provincial Legislation

In addition to federal initiatives, Ontario and Québec are actively working on their own AI-related legislation.

- **Ontario's Bill 194:** Also known as the Strengthening Cyber Security and Building Trust in the Public Sector Act, this bill enhances AI governance and data privacy in public sector entities. https://www.ipc.on.ca/en/media-centre/blog/bill-194-ontarios-missed-opportunity-lead-ai and Bill 194, Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024 - Legislative Assembly of Ontario
- **Amendments to Québec's Privacy Laws (Law 25):** Québec is revising its privacy laws to better accommodate the challenges posed by AI technologies. The amendments modernize privacy laws to address AI challenges, including stricter consent requirements and greater transparency for individuals on how their data is used. Law 25: Québec's second wave of new privacy amendments is here : Clyde & Co

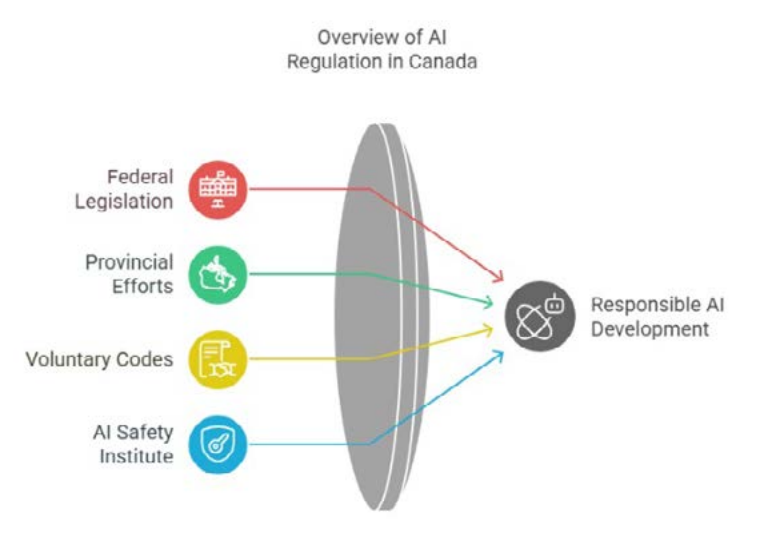
A Newest Developments (Federal)

Canadian Artificial Intelligence Safety Institute (CAISI) Launched in late 2024, the Canadian Artificial Intelligence Safety Institute (CAISI) focuses on mitigating safety risks and promoting responsible AI development. It provides guidance, resources, and oversight to ensure AI technologies are developed and deployed safely and ethically. CAISI also collaborates with international partners to advance research and practices in AI safety. https://cifar.ca/cifarnews/2024/11/12/government-of-canada-announces-canadian-ai-safety-institute/

Canada is actively shaping regulations to ensure AI serves public needs safely and fairly. As an educator, you might find these points relevant:

- **Bill C-27:** These laws ensure accountability and transparency in AI. For you, this means having the right to know how an AI tool is using your learners' data and ensuring the tools you use adhere to ethical standards, such as safeguarding privacy and preventing misuse of sensitive information. This enables you to make informed decisions about integrating AI into your teaching practices, enhancing the learning experience while upholding your learners' trust.
- **Voluntary Code of Conduct & CAISI:** More than policies, these frameworks are reminders to critically assess every new tool. Before integrating an AI application in your classroom, ask these questions:

1. How does it safeguard my learners' privacy?
2. Does it ensure transparency in its operations, and align with ethical standards like fairness and accountability?



The Canadian AI Regulatory Landscape, Tailored for LBS

Why Ethical AI matters?

- ✓ **Building Trust with Learners:** Many adult learners may have had negative experiences with institutions. Transparent and ethical AI practices can help build trust.
- ✓ **Respecting Life Stories:** Adult learners bring rich personal histories to the classroom. Ethical AI practices ensure their sensitive data isn't just another statistic, but is handled with care that respects their life experiences.
- ✓ **Enhancing Learning Outcomes:** Responsible AI can offer personalized learning pathways, but only when data is used appropriately enhancing both the educational journey and real-world opportunities

Imagine discussing with your learners how a new software not only personalizes their reading material but also details who sees their progress data and why it matters. Real stories like this spur interest and bring regulations to life.

Six Actionable Steps for the Adult Educators

1. Audit Your AI Tools

Perform a hands-on review of every digital tool you use—from assessment generators to multimedia apps. Consider these questions:

- **Data Collection:** What information does the tool need from your learners?
- **Storage & Access:** Where does the data go, and who can see it? Think of it as checking the locks on a door in a Your organization
- **Retention Policies:** How long is learner data kept, and why?

> **TIP:** Request a report from your vendors. Many reputable providers can share insights into their data practices.

2. Implement Data Minimization

Focus on gathering only what you need:

- **Define Clear Objectives and Reasoning for its use:** Before introducing a tool, ask if every data point is aligned with your learning outcomes. Imagine a new AI tool claims to improve learner's engagement but collects personal data. How do you decide whether to use it in your classroom?
- **Regular Clean-Ups:** Periodically check your systems to remove unnecessary data.
- **Keep it Simple:** Document in plain language the purpose behind each data element—this transparency is key to mutual trust.

3. Foster Transparency in the Classroom

Engage your learners in conversations around technology use:

- **Discuss AI's Role:** Explain in everyday language how AI tools work for their benefit.
- **Relate to Real Life:** For example, show how data helps adapt learning to their needs—not to survey or judge them.
- **Cultivate Ownership:** Empower learners by letting them know they can ask questions or request that certain data be deleted.

4. Integrate AI Literacy into Your Curriculum

Your learners already engage with technologies daily. Incorporate discussions that highlight:

- **Practical Applications:** How is AI used in job applications, personal finance, or healthcare? See AI Bytes 4 for info.

- **Evaluating Tools:** Teach them to spot bias or "black box" decision-making in everyday apps. Check out this fantastic resource from Media Smarts to help learn understand how the black box works: Unpacking the Black Box: Explaining Algorithms and AI
- **Ethical Use:** Use classroom debates, case studies, or role-playing scenarios to discuss ethical dilemmas around data use. The following student data privacy and data ethics scenarios are free, supplemental course materials that aim to help educators understand privacy risks and ethical data. See Student Data Privacy and Data Ethics Scenarios (page 192) for a great activity on implications related to Facial Recognition.

Consider a session where learners compare a traditional literacy tool with an AI-powered peer review system, discussing benefits and risks side by side.

5. Set Up Ongoing Governance Procedures

Streamline ethical AI usage into daily practices:

- **Create Clear Policies:** Work with your organization to design policies to guide the selection and use of AI tools.
- **Review Regularly:** Schedule periodic reviews of your digital tools to ensure they still align with ethical standards and evolving regulations.
- **Have an Incident Plan:** Develop a straightforward process for addressing any data breaches or ethical concerns, ensuring your learners feel supported and heard.

6. Inclusivity & Cultural Responsiveness

Adult education isn't just theory—it's lived experience. Share stories of learners who benefited from adaptive learning programs that respected their privacy, or discuss challenges posed by mismanaged data that could affect employment opportunities

- **Cultural Nuances:** Consider how AI tools might overlook local dialects or cultural context.
- **Accessible Platforms:** Choose tools that are easy for everyone to use, especially for students who might not be confident with technology or technical language.
- **Indigenous and other diverse perspectives:** Empower learners from marginalized backgrounds by ensuring they have agency over their data. Celebrate Indigenous perspectives by valuing data sovereignty and honoring traditional ways of knowing and teaching. Extend this respect to all communities to build an inclusive and equitable digital environment where everyone can thrive together.

10 Actionable Steps for Organizations

Understanding the Privacy Risks Introduced by AI

AI's transformative potential in adult education is undeniable, yet its ethical implementation demands careful navigation. Organizations must proactively address the complex landscape of opportunities and challenges, balancing innovation with fairness, transparency, and equity. This includes safeguarding privacy, ensuring inclusivity, building trust, and aligning technology with teaching goals.

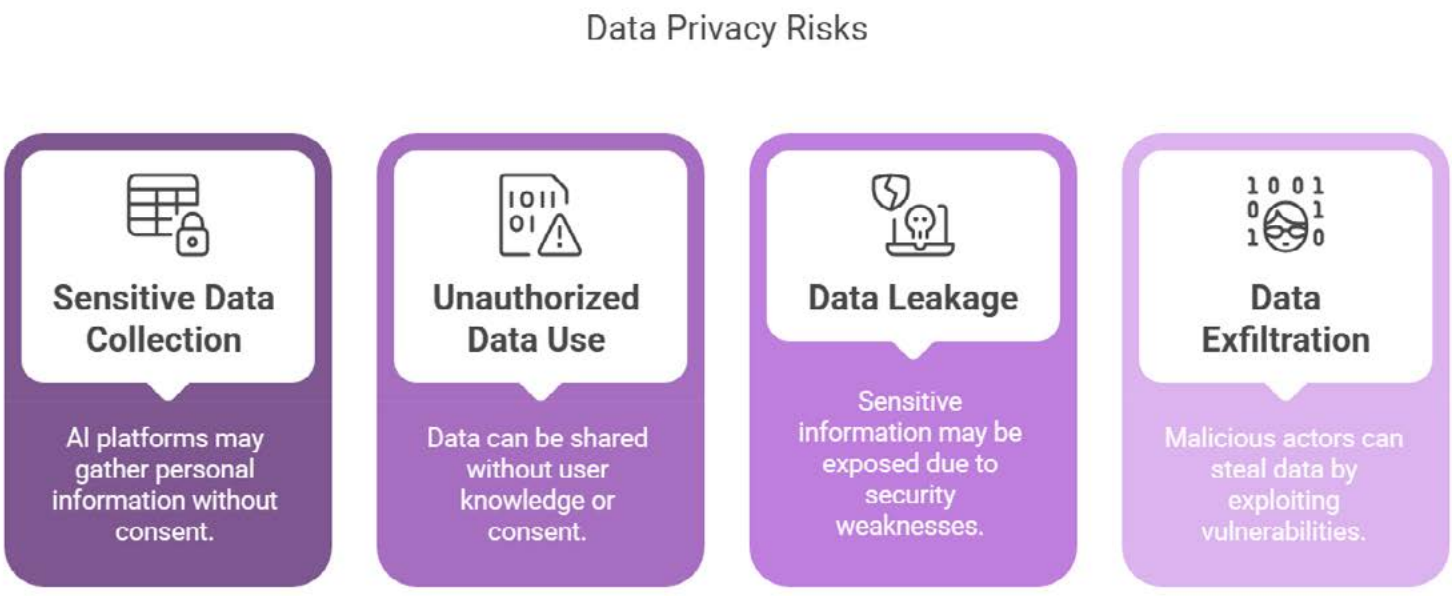
Simultaneously, we must recognize that AI's pervasive integration into our lives necessitates a heightened focus on privacy. Beyond the algorithms that drive personalized experiences and automation, we must prioritize safeguarding personal and organizational data. This requires vigilance against data collection risks, user profiling, and potential security breaches.

In essence, responsible AI adoption demands a dual commitment: organizational action for ethical implementation and a proactive approach to protecting privacy.

To guide this process, here are 10 actionable steps safeguard Learner Privacy and build ethical AI practices with examples for organizations:

1. Prioritize Ongoing Professional Development

- **Workshops and Training:** Schedule recurring sessions for educators to explore AI fundamentals, ethical data use, and privacy concerns. Include practical activities like hands-on projects, role-playing exercises (e.g., simulating ethical dilemmas), and expert talks to enrich learning.
- **Peer Collaboration:** Foster study circles and communities of practice where educators exchange experiences, analyze research, and discuss AI's implications. These forums can encourage innovation while addressing challenges collaboratively.
- **Certification Opportunities:** Recommend accessible, high-quality online courses or certifications focused on AI ethics, digital literacy, and compliance with privacy regulations. These resources ensure educators stay ahead in a rapidly changing field.



2. Enhance Transparency and Communication

- **Plain-Language Documentation**: Develop easy-to-understand guides or infographics explaining how AI tools work, what data is collected, and why it's necessary. This helps demystify any "black box" issues and builds trust with learners.
- **Data Use Contracts & Consent Forms**: Create straightforward consent forms that clarify what data is collected and how it will be used. Listen to learners' questions and update these documents as technologies change.
- **Interactive Demonstrations:** Use real-life examples or interactive digital demonstrations in your curriculum. For instance, a short demo showing how data influences personalized learning can help learners see the benefits—and limits—of AI.

3. Support Educators to build Digital Literacy & AI Ethics into the Curriculum

- **Case Studies & Role-Playing:** Bring real-world dilemmas into the classroom by discussing case studies that highlight ethical challenges in AI. This might involve simulated scenarios where learners analyze different outcomes based on varying data practices.
- **Student-Driven Projects:** Have learners research and present on how AI is used in everyday technologies, encouraging them to critically evaluate the biases and ethical implications. This empowers them to be both informed users and future advocates.
- **Ethics Debates & Reflection Sessions:** Host structured debates on the pros and cons of AI in literacy education. These sessions not only foster critical thinking but also provide insights into learner concerns that you can address in your practices.

4. Implement Robust Data Auditing and Minimization Practices

- **Regular Audits:** Schedule periodic reviews of the digital tools and platforms you use. Evaluate which data points are essential for achieving learning outcomes and remove any superfluous information.
- **Vendor Checklists:** Develop a checklist for selecting and evaluating AI tools that covers data privacy features, transparency of algorithms, and compliance with local and national regulations.
- **Documented Data Flows:** Maintain clear records of where learner data goes—from collection to storage, access, and eventual deletion. This not only aids compliance but also reinforces accountability.

5. Mitigate Bias and Champion Inclusivity

- **Bias Training:** Equip educators with dedicated sessions focused on identifying potential biases in AI systems. This training should cover both technical and cultural considerations adapted to diverse adult learner populations.
- **Diverse Data Involvement:** Involve a wide range of learner voices when selecting or reviewing AI tools, ensuring that underrepresented groups' feedback is integral to the decision-making process.
- **External Evaluations:** When possible, partner with third-party auditors or institutions that can provide an objective review of your AI tools and recommend adjustments that better serve all learners.

6. Develop Adaptive Governance and Policy Frameworks

- **Collaborative Policy Development:** Work with your institution's leadership to develop internal policies that are flexible enough to adapt to rapidly evolving regulations and technological advancements. Engage

stakeholders (administrators, IT staff, and learners) in this process.

- **Regulatory Updates:** Subscribe to newsletters or forums that monitor changes in AI policies—this arms you with the knowledge needed to revise your practices promptly.
- **Crisis Management Planning:** Having a clear, well-documented plan in place for responding to data breaches or ethical lapses can reassure staff and learners, further solidifying trust in your institutional practices.

7. Address Resource Constraints Through Collaboration

- **Shared Resources & Networks:** Collaborate with other educational institutions or adult education centres to pool resources, share successful strategies, and even co-develop materials on ethical AI.
- **Funding & Grants:** Research educational grants and funding opportunities specifically aimed at improving digital learning infrastructures. These funds can often help offset the costs of implementing best practices.
- **Leveraging Open-Source Tools:** When budgets are tight, consider reliable open-source AI tools that adhere to strong ethical guidelines. Ensure these tools are regularly evaluated against your organization's update needs and ethical standards.

8. Human Oversight and Accountability

To counteract AI's "black box" problem:

- **Review Protocols:** Introduce educator-led reviews of AI-driven decisions to maintain accountability.
- **Feedback Mechanisms:** Create channels for continuous feedback from educators and learners, ensuring iterative improvements.

9. Cybersecurity Measures

Reinforce data protection by:

- **Vulnerability Assessments:** Conduct regular evaluations to prevent unauthorized access.
- **Secure Infrastructure:** Implement robust incident response protocols to address potential breaches.
- **Opt for Enterprise Data Protection (EDP):** If you're using AI tools in a business context, consider services like EDP. This option typically includes robust measures such as data encryption (both at rest and in transit), data isolation, and guarantees that data from prompts and responses won't be used to train general-purpose models.
- **Utilize Data Masking and Pseudonymization:** Apply data masking techniques to obscure sensitive information. Replace private identifiers with fictitious ones (pseudonymization) to limit the exposure of personal details.

Examples:

Data Masking:

- Original Data: A credit card number such as 1234-5678-9876-5432.
- Masked Data: XXXX-XXXX-XXXX-5432. The first 12 digits are hidden to obscure the sensitive information, but the last 4 digits are left visible for identification purposes.

Pseudonymization:

- Original Data: A name like "John Smith" and their email "john.smith@example.com".
- Pseudonymized Data: Replace these with fictitious identifiers such as "User12345" and "user12345@domain.com". This ensures the individual cannot easily be identified without additional information.

10. Holistic Engagement and Impact Assessment

For a comprehensive approach:

- **Community Collaboration:** Involve educators, developers, policymakers, and community members to foster trust in AI integration.
- **Ethical Audits**: Periodically evaluate the social impact of AI tools, ensuring they remain beneficial and fair.
- **Risk Management:** Identify and mitigate potential new risks to stay proactive in AI adoption.

Your Next Three Steps:

✓ Join the conversation! New AI professional development sessions are coming to your mailbox. It's the perfect place to connect, share best practices, and learn together.

✓ Request support to the organizations where you and your learners explore new AI tools together. Some organizations that can assist with connections: Contact North | Contact Nord and AlphaPlus.

✓ Stay informed: Follow updates from the Canadian Artificial Intelligence Safety Institute and Digital Governance Council - By integrating ethical AI practices into your teaching strategy, you reinforce the values of respect, empowerment, and lifelong learning. This proactive stance not only protects your learners but also enhances the very fabric of adult education—trust, transparency, and transformation.

Thank you for investing your time in exploring AI ethics and its impact on adult education. By using AI thoughtfully and responsibly, you create a learning environment where trust flourishes and opportunities abound. We hope this guide provided practical insights and encourages you to continue exploring the exciting possibilities of AI in your work. Let's move forward, united in our commitment to ensuring AI empowers every learner, leaving no one behind.

References

https://ised-isde.canada.ca/site/ised/en/canadian-artificial-intelligence-safety-institute

AI regulation in Canada: New laws and regulations to know | Canadian Lawyer

Canadian Artificial Intelligence Safety Institute

Law 25: Québec's second wave of new privacy amendments is here : Clyde & Co

Consumer Privacy Protection Act

The Artificial Intelligence and Data Act (AIDA) – Companion document

Data Privacy In AI-Driven Learning And Ethical Considerations - eLearning Industry