AI & CYB: Artificial Intelligence and Cybersecurity Literacy Needs of Canadian Students

Muhammad Ali Nadeem
St. Clair College, Windsor, ON, Canada, ali.nadeem@trios.com
Bishwo Prakash Pokharel
triOS College, Toronto, ON, Canada, bishwo@crnglobal.ca

Abstract - **Artificial intelligence and cybersecurity have become essential elements of digital literacy in modern education, influencing how students access information, collaborate, and engage online. In Ontario's schools, learners routinely use AI-enabled platforms, automated feedback systems, and a growing ecosystem of digital applications. However, frequent interaction does not necessarily translate into meaningful understanding. Many students display confidence with everyday digital tasks, yet this familiarity often conceals limited awareness of how AI systems function, what their constraints are, and how algorithmic decisions shape their online experiences. Cybersecurity knowledge shows similar inconsistencies. Students may know how to create passwords or avoid obvious phishing attempts, but they often struggle to recognize more sophisticated threats, interpret data-privacy risks, or critically assess the credibility of digital content. These gaps highlight the need for structured learning experiences that extend beyond technical skills and foster deeper analytical thinking, ethical awareness, and responsible digital citizenship. The study emphasizes the importance of embedding AI and cybersecurity literacy more deliberately within Ontario's curriculum. Strengthening teacher training, incorporating real-world scenarios, and aligning instructional practices with rapidly evolving technologies can help students build the competencies required for safe, informed participation in digital environments. The paper concludes with targeted recommendations for educators, school leaders, and policymakers to support a coherent, province-wide strategy for enhancing AI and cybersecurity literacy across K–12 education.**

Index Terms – Artificial Intelligence, Cybersecurity, Digital Literacy, Ontario Education.

INTRODUCTION

The rapid integration of artificial intelligence (AI) and digital technologies into daily life has transformed the skills required for students to participate safely and effectively in modern society. Ontario's education system is increasingly shaped by AI-powered tools, digital learning platforms, and online communication environments. As a result, AI literacy and cybersecurity literacy have emerged as critical competencies for students [7][11][16]. Understanding students' current literacy levels is essential for designing effective curriculum interventions and ensuring equitable access to digital skills.

The purpose of this paper is to assess AI and cybersecurity literacy levels among Ontario students, identify learning needs, and propose recommendations for curriculum development & policy. This analysis draws on existing research, digital literacy frameworks, and emerging trends in educational technology.

I. *Artificial Intelligence (AI) Literacy*

AI literacy refers to the knowledge, skills, and attitudes required to understand, evaluate, and responsibly use AI systems. Scholars typically define AI literacy as including conceptual understanding, critical evaluation, ethical awareness, and practical application [6]. AI literacy captures the blend of knowledge, skills, and attitudes that individuals need to make sense of artificial intelligence and use it responsibly. It goes beyond simply knowing what AI is; it involves understanding how these systems work, being able to critically evaluate their outputs, and recognizing the ethical implications of their use. Scholars emphasize that true AI literacy requires both conceptual understanding—such as how algorithms make decisions—and practical application, including the ability to interact with AI tools thoughtfully and safely. By developing these competencies, learners are better equipped to navigate an increasingly AI-shaped world with confidence and judgement [7]. AI key components include:

- Understanding how AI systems make predictions
- Recognizing AI in everyday technologies
- Identifying algorithmic bias and misinformation
- Using AI tools responsibly in academic contexts

II. *Cybersecurity (CYB) Literacy*

Cybersecurity literacy encompasses the ability to recognize digital threats, protect personal information, and practice safe online behaviors. Cybersecurity literacy encompasses far more than basic technical know-how — it reflects a broad set of competencies that enable individuals to navigate digital environments safely and confidently. At its core, it involves the ability to recognize common digital threats such as phishing attempts, malware, social engineering, and suspicious online activity. It also requires understanding how

to protect personal information by using strong passwords, enabling multi-factor authentication (MFA), managing privacy settings, and making informed decisions about what data to share online [8].

Equally important is the development of safe online habits, including evaluating the credibility of websites, avoiding risky downloads, and maintaining awareness of how digital actions can expose vulnerabilities. When students build these skills, they are better equipped to participate in digital spaces responsibly, reduce their risk of harm, and contribute to a more secure online community. Hence, cybersecurity includes:

- Awareness of phishing, scams, and social engineering
- Understanding digital footprints and privacy settings
- Using strong authentication practices
- Knowing how to respond to security incidents

ONTARIO CONTEXT

Ontario's curriculum includes digital literacy elements, but AI and cybersecurity competencies are not yet standardized across all grades. School boards vary in implementation, teacher training, and access to technology. This variability underscores the need for a province-wide assessment of student competencies [1].

Ontario's curriculum embeds digital literacy as a core transferable skill across Grades 1–12, emphasizing students' ability to use technology safely, legally, and ethically. The Ministry defines digital literacy as the capacity to "*solve problems using technology in a safe, legal, and ethically responsible manner*," while also engaging with data literacy and emerging technologies. This vision also extends to data literacy and emerging technologies, ensuring that students learn to interpret, question, and apply data while understanding the implications of rapidly evolving digital systems. By embedding these expectations across all subject areas, the curriculum aims to cultivate learners who are not only competent users of technology but thoughtful, informed, and ethical digital citizens [5].

At the primary level, digital literacy outcomes are integrated into Language, Science and Technology, and Social Studies, with a growing emphasis on digital media literacy—particularly in the updated Language curriculum, which highlights the need for students to differentiate between accurate information and misinformation in digital environments. Resources such as MediaSmarts' *Building Blocks of Digital Media Literacy* support early-grade teachers in meeting these expectations by aligning activities with Ontario's curriculum outcomes for Kindergarten to Grade 3. Despite these structured expectations, competencies related specifically to artificial intelligence and cybersecurity remain inconsistently addressed, as they are not formally standardized across all primary grades.

Digital literacy in secondary education is treated as a transferable competency that students must demonstrate across all subjects. Learners are expected not only to use digital tools but to choose technologies purposefully to support collaboration, communication, creativity, and problem solving [4]. This reflects Ontario's broader shift toward preparing students for complex digital environments that demand fluency, adaptability, and responsible judgment. Research shows adolescents benefit most when they learn to assess a tool's purpose, limitations, and ethical implications— an approach aligned with Ontario's competency-based model. As students advance through secondary grades, they increasingly integrate digital platforms into inquiry, group work, and creative tasks, reinforcing digital literacy as both a practical skill and a cognitive discipline.

Digital media literacy is particularly prominent within English courses from Grades 7–12, where students engage with a wide range of multimodal texts, including videos, social media content, interactive websites, and digital narratives. The curriculum requires students to analyze how meaning is constructed through visual, auditory, and interactive elements, and to examine how digital media shapes public opinion, identity, and cultural norms [17]. This emphasis aligns with contemporary research showing that youth are frequent consumers of online content but often lack the critical frameworks needed to assess credibility, detect bias, or recognize persuasive design techniques.

By embedding digital media literacy into English instruction, Ontario aims to cultivate students who can navigate online information ecosystems with discernment — evaluating sources, questioning algorithms, and understanding how digital platforms influence communication. This integrated approach positions students to become thoughtful, critical participants in a rapidly evolving digital world.

At the secondary level, digital literacy continues as a mandated transferable skill, requiring students to select and use appropriate digital tools to collaborate, communicate, create, and solve problems. Digital media literacy is deeply embedded in English courses from Grades 7–12, where students are expected to analyze multimodal texts, understand the influence of digital media, and critically evaluate online information sources [19].

The curriculum explicitly acknowledges the impact of emerging technologies on communication and stresses the importance of independent critical thinking in digital contexts. However, while digital literacy is well-represented, competencies in AI awareness, algorithmic bias, data ethics,

and cybersecurity practices are not uniformly integrated across secondary subjects or grade levels. School boards differ significantly in how they implement digital literacy instruction, the extent of teacher training, and the availability of technological resources, leading to uneven student experiences across the province [26]. This inconsistency reinforces the need for a province-wide assessment of digital, AI, and cybersecurity competencies to ensure equitable skill development for all Ontario learners aged 18 or younger [17].

METHODOLOGICAL APPROACH

A comprehensive evaluation of AI and cybersecurity literacy generally requires drawing on a broad set of data-gathering approaches, using several complementary methods to capture knowledge, skills, behaviors, and real-world application:

I. *Surveys and Questionnaires*

Surveys can measure students' conceptual knowledge, confidence levels, and self-reported behaviors. Scenario-based questions help assess decision-making in realistic digital situations. Ontario has conducted surveys related to students' digital literacy, technology use, and digital learning experiences, but these surveys have primarily focused on postsecondary students, not K–12 learners. The available surveys measure students' confidence with digital tools, their self-reported behaviors, and their experiences with technology-enabled learning, but they do *not* directly assess AI literacy or cybersecurity competencies for students aged 18 or younger.

The latest publicly available findings from eCampusOntario's *Digital Learning Experiences Survey* do not measure students' AI literacy or cybersecurity knowledge, and they do not assess digital literacy skills directly. Instead, the survey focuses on students' *experiences* with digital learning—such as satisfaction, access to technology, and challenges—not their conceptual understanding or technical competencies [27].

The most recent Ontario-specific data comes from the 2023 Ontario Report and the 2024–2025 CDLRA Pan-Canadian Digital Learning Trends, which emphasize institutional perspectives rather than student skill assessments [28][29]. The 2023 Ontario Report, produced by the Canadian Digital Learning Research Association (CDLRA) in partnership with *eCampusOntario*, summarizes trends in digital learning across Ontario's postsecondary sector. However, it does not include measures of students' digital literacy proficiency, nor does it test their knowledge of AI or cybersecurity. The report is based on institutional staff responses, not student skill assessments. What it does report:

- Institutions expect increased technology use in postsecondary education.
- There is a need for more professional development, technology infrastructure, and policies for digital learning.

- Educators report high confidence in teaching online or hybrid courses (e.g., 91% feel they have the skills to teach partially online).

These findings relate to teaching capacity - not student digital literacy [27].

II. *No AI or Cybersecurity Knowledge Assessment*

Across the major reports reviewed — the 2023 Ontario Report, the 2024/2025 *Pan-Canadian Digital Learning Trends* studies, and the *eCampusOntario* infographic—there is a consistent absence of data on what students actually know about artificial intelligence or cybersecurity [27].

None of these documents include assessments of AI literacy, cybersecurity knowledge, or students' conceptual understanding of emerging technologies. Instead, their focus remains largely system-level: institutional readiness, educator digital competencies, infrastructure capacity, and broad trends in online or hybrid learning. While these areas are important for understanding the digital learning landscape, they do not provide insight into whether students themselves are developing the foundational skills needed to navigate AI-driven tools or protect themselves in increasingly complex digital environments [7]. As a result, policymakers and educators lack the evidence required to evaluate student preparedness in these rapidly evolving domains.

Even when student perspectives appear in the available research, they do not address digital literacy competencies. The 2025 Pan-Canadian Report, which incorporates student-focused insights from Academica Group, highlights issues such as preferences for flexible learning formats, challenges related to access and connectivity, and levels of satisfaction with online learning environments. These findings help illuminate students' experiences with digital learning but stop short of measuring their understanding of AI systems, their ability to critically evaluate algorithmic outputs, or their awareness of cybersecurity risks.

Without direct assessment of these competencies, Ontario and Canadian education systems are left with an incomplete picture—one that captures how students feel about digital learning, but not what they actually know or can do in relation to emerging technologies [8]

III. *Ontario Postsecondary Data Gap*

Ontario currently has no province-wide postsecondary survey that directly measures students' digital literacy proficiency, AI literacy, cybersecurity understanding, or their underlying conceptual knowledge and skill levels. While individual institutions may conduct small-scale assessments or course-level evaluations, there is no standardized, system-wide instrument that captures how well students understand emerging technologies, algorithmic systems, data practices, or digital risk [30].

This absence of coordinated measurement means policymakers and institutions lack reliable evidence about students' actual competencies, misconceptions, or preparedness for an AI-driven economy. It also limits the province's ability to identify equity gaps, track progress over

time, or design targeted interventions that strengthen students' digital and cybersecurity capabilities.

Existing surveys in Ontario's postsecondary sector focus primarily on broader digital learning experiences rather than student competencies. Reports such as the Pan-Canadian Digital Learning Survey examine institutional readiness, educator confidence, technology adoption patterns, and student experiences with online or hybrid learning environments—not their literacy or skill levels in AI, cybersecurity, or digital problem-solving [29]. These surveys provide valuable insights into infrastructure, pedagogical trends, and faculty development needs, but they do not assess whether students can critically evaluate AI systems, recognize cyber threats, or apply digital tools effectively and ethically.

As a result, Ontario's current data landscape captures how technology is used in postsecondary education, but not how well students understand or navigate it—highlighting a significant gap that future research and policy must address. Therefore, it can be reasonably concluded that Ontario currently lacks any province-wide postsecondary survey that measures:

- Digital literacy proficiency
- AI literacy
- Cybersecurity understanding
- Students' conceptual knowledge or skill levels

The existing surveys measure:

- Experiences with digital learning
- Institutional readiness
- Educator confidence
- Technology use trends

This indicates that Ontario currently lacks systematic data on students' digital, AI, and cybersecurity competencies, underscoring the need for the development of new assessment tools.

IV. *Performance Based Tasks*

Performance tasks provide insight into students' applied skills, such as identifying phishing attempts or evaluating AI-generated content. Performance-based tasks offer one of the most authentic and informative ways to assess Ontario students' AI and cybersecurity knowledge because they capture how learners apply concepts in real-world scenarios rather than simply recalling definitions. In the context of cybersecurity, these tasks might involve asking students to analyze a simulated inbox and identify increasingly sophisticated phishing attempts, evaluate the security of sample passwords, or determine the safest response to a suspicious message [31].

For AI literacy, performance tasks could require students to compare human-written and AI-generated content, identify signs of algorithmic bias in a dataset, or critique the reliability of outputs from a generative AI tool. These activities reveal not only what students know but how they think—highlighting their reasoning processes, misconceptions, and decision-making strategies. Because AI and cybersecurity

threats evolve rapidly, performance-based assessments help educators understand whether students can transfer their learning to unfamiliar situations, a skill that traditional tests often fail to measure.

Performance-based tasks support equitable data collection by offering multiple entry points for students with diverse learning styles, language backgrounds, and levels of digital access. When paired with surveys, interviews, and digital analytics, they create a fuller picture of student competencies. Surveys capture confidence and self-reported behaviors, interviews reveal attitudes and ethical concerns, and analytics show how students interact with AI tools or respond to simulated threats [32]. Together, these methods allow Ontario to triangulate findings, ensuring that assessments reflect both students' conceptual understanding and their practical abilities.

By integrating performance-based tasks into a broader, province-wide data collection strategy, Ontario can generate actionable insights that inform curriculum updates, teacher training, and system-level policy development. These tasks help identify where students excel—such as recognizing obvious scams or navigating digital platforms—and where they struggle, such as detecting subtle phishing cues, understanding algorithmic bias, or evaluating AI-generated misinformation. This richer, multidimensional data enables policymakers and educators to design targeted interventions, allocate resources more effectively, and ensure that all students develop the AI and cybersecurity competencies needed to thrive in a rapidly evolving digital world. Ontario has not collected student data through performance-based tasks specifically measuring AI or cybersecurity knowledge in recent years. There could be several well-supported, research-aligned reasons why Ontario may not have collected student data through performance-based tasks measuring AI or cybersecurity knowledge in recent years:

1. Lack of established assessment frameworks AI literacy and cybersecurity competencies are emerging domains, and there are no widely adopted, validated K–12 assessment tools in Canada. Without standardized rubrics or benchmarks, provinces often hesitate to implement large-scale performance-based evaluations [33].

2. Rapid evolution of technology AI systems, digital tools, and cyber threats evolve faster than curriculum cycles. Designing performance tasks that remain relevant, accurate, and pedagogically sound is challenging when the underlying technologies shift every year.

3. Limited educator training and capacity Teachers often report low confidence in teaching AI concepts or cybersecurity skills. Without strong professional development, implementing performance-based assessments—especially those requiring technical judgment—is difficult to scale across the province [30].

4. Infrastructure and resource constraints Performance-based digital assessments require secure devices, controlled environments, and technical support. Many schools face

inconsistent access to technology, making province-wide implementation inequitable or impractical.

5. Policy focus on broader digital literacy rather than specific competencies Ontario's curriculum emphasizes general digital literacy and safe technology use, but does not mandate explicit measurement of AI or cybersecurity knowledge [21]. As a result, system-level data collection has not been prioritized.

6. Privacy and security considerations Assessing cybersecurity skills can involve simulated threats, system vulnerabilities, or network tasks. Provinces may avoid such assessments due to concerns about student data protection, misuse of tools, or unintended exposure to sensitive content.

However, a more complete understanding—based on publicly available information about provincial assessments, ministry initiatives, and board-level practices—indicates that: Ontario has *not* implemented any province-wide, performance-based assessments that evaluate K–12 students' AI literacy, cybersecurity skills, or their ability to apply these concepts in real-world scenarios. The Ministry of Education's large-scale assessments (e.g., EQAO) do not include tasks related to identifying phishing attempts, evaluating AI-generated content, recognizing algorithmic bias, or responding to cybersecurity incidents. Likewise, no publicly released provincial reports indicate that school boards have been required to administer hands-on or scenario-based tasks to measure students' applied competencies in these areas [30].

Some local or pilot initiatives may exist—such as classroom-level activities, board-developed digital citizenship modules, or extracurricular cybersecurity competitions—but these are not standardized, not province-wide, and not used for systematic data collection. They also vary widely by school board, depending on teacher expertise, available technology, and local priorities. Importantly, none of these initiatives have produced publicly available, large-scale datasets that assess students' applied AI or cybersecurity knowledge through performance-based tasks. This means Ontario currently lacks empirical, skills-based data on how well students can:

- Detect phishing or social engineering attempts
- Evaluate AI-generated misinformation
- Identify algorithmic bias
- Apply data-privacy practices
- Respond to cybersecurity incidents

The absence of such data is one of the strongest arguments for developing a province-wide assessment framework that includes performance-based tasks, since these tasks reveal students' real-world decision-making and practical competencies far more effectively than surveys or self-reports.

FOCUS GROUPS AND INTERVIEWS

Qualitative methods capture students' attitudes toward AI, perceptions of online risk, and real-world digital habits.

Focus groups and interviews offer Ontario an essential qualitative lens for understanding students' AI and cybersecurity knowledge because they reveal the *why* behind students' behaviours, perceptions, and decision-making in ways that surveys or tests cannot. Through guided discussions, students can articulate their attitudes toward AI—whether they view it as helpful, risky, confusing, or exciting—and explain how they actually use AI tools in schoolwork, social media, and daily life. These conversations also uncover students' *perceptions of online risk*, including what they consider dangerous, what they ignore, and how they judge the credibility of digital content.

Importantly, qualitative methods shed light on real-world digital habits that are often invisible in formal assessments, such as how students manage passwords, respond to suspicious messages, or rely on AI for homework. Focus groups and interviews can also surface misconceptions, ethical concerns, and emotional responses—fear, overconfidence, curiosity—that shape how students interact with technology. When combined with performance-based tasks and quantitative surveys, these qualitative insights help Ontario build a more complete, nuanced understanding of students' AI and cybersecurity readiness, ensuring that future curriculum and policy decisions reflect the lived experiences of learners across the province.

Ontario has not conducted any province-wide focus groups or interviews with K–12 students specifically to assess their AI literacy or cybersecurity knowledge. There is no Ministry-led initiative, no EQAO-related study, and no publicly released school-board-level report that uses qualitative methods to systematically gather student perspectives on AI, online risk, digital ethics, or cybersecurity behaviours.

I. No Province-wide Qualitative Data Exists for K-12

There are no documented focus groups or interviews conducted across Ontario schools that examine:

- Students' understanding of AI
- Their perceptions of algorithmic bias
- Their awareness of cybersecurity threats
- Their real-world digital habits
- Their ethical concerns about generative AI

This means Ontario lacks qualitative insight into how students *feel* about AI, how they *interpret* online risks, or how they behave in digital environments.

II. Small-scale or Local Initiatives Exist, but Not Standardized

Individual teachers, schools, or research teams may have run:

- Classroom discussions
- Small research projects
- Pilot studies
- Board-specific digital citizenship consultations

However, these are:

- Not province-wide

- Not coordinated
- Not publicly reported as formal data collection
- Not focused specifically on AI or cybersecurity literacy

They also do not produce consistent, comparable data across Ontario.

III. *Postsecondary Institutions – not K12 – Conducted Qualitative Studies*

Ontario universities have conducted studies on digital literacy and AI use, but these focus on postsecondary learners rather than children or youth. The province lacks systematic qualitative data—such as focus groups or student-centered inquiry—on K–12 students' AI literacy, cybersecurity understanding, or perceptions of digital risk [11]. This gap highlights the need for a coordinated strategy to capture student voice for curriculum and policy development. Research across Canada and internationally shows that young people often use AI tools without understanding how they work and frequently overestimate their cybersecurity skills, reinforcing the urgency for Ontario to develop robust, student-informed assessment tools.

### IV. *Digital Simulations*

Gamified cybersecurity challenges and AI ethics simulations offer authentic contexts for assessing higher-order thinking. Based on all publicly available information, Ontario has not collected any province-wide student data using digital simulations to assess AI or cybersecurity knowledge in recent years. No Ministry of Education initiative, EQAO assessment, or system-level research project has used simulation-based tasks to evaluate how K–12 students respond to phishing attempts, analyze AI-generated content, detect algorithmic bias, or navigate digital security scenarios.

Digital simulations—such as mock phishing environments, sandboxed cybersecurity challenges, or interactive AI decision-making tools—are widely recognized as powerful assessment methods, but Ontario has *not implemented them at scale* for data collection or curriculum monitoring. Some isolated or small-scale activities may occur at the classroom or school-board level, such as:

- Cybersecurity competitions (e.g., CyberPatriot-style events)
- Teacher-created simulations for digital citizenship lessons
- Board-specific pilots exploring online safety modules

However, these efforts are not standardized, not province-wide, and do not produce publicly reported datasets about students' applied AI or cybersecurity competencies. They also vary significantly depending on teacher expertise, available technology, and local priorities, meaning they cannot be considered systematic data collection. In short, Ontario currently lacks simulation-based evidence about how students actually behave when confronted with realistic digital threats or AI-generated content. This gap highlights a

major opportunity: digital simulations could become a cornerstone of future assessment strategies, offering rich, authentic insights into students' real-world readiness in AI and cybersecurity.
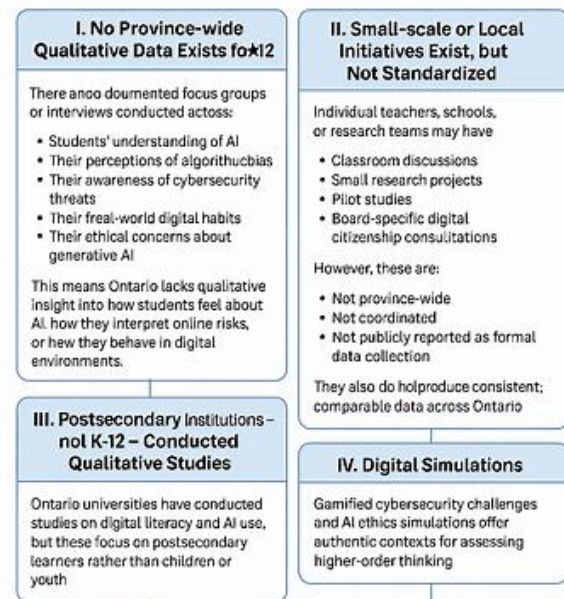
THE GENERAL FINDINGS

I. *The Situation*

In the absence of comprehensive, province-wide data collection methods to assess students' AI and cybersecurity learning levels, Ontario faces significant challenges in generating reliable empirical insights and drawing meaningful conclusions.

Without standardized tools such as performance-based tasks, digital simulations, focus groups, or qualitative interviews, it becomes difficult to measure students' applied competencies, conceptual understanding, and real-world digital behaviors. To compensate for this gap, fragmented efforts have emerged across the province, including classroom-based digital simulations led by individual teachers, school board-specific pilot programs exploring online safety, and cybersecurity competitions that offer limited snapshots of student skills.

Additionally, some financial institutions have begun educating teenage customers on cybersecurity and information privacy, contributing informal data points that reflect broader awareness trends. However, these isolated initiatives lack consistency, scalability, and integration into a unified assessment framework, making it cumbersome to synthesize findings or inform policy and curriculum development at the provincial level.

II. *Strengths*

However, Ontario students increasingly show a strong baseline of digital readiness, reflected in their growing familiarity with AI-enabled tools, comfort navigating digital platforms, and rising interest in AI-related career pathways. In classrooms and everyday life, students routinely interact

with AI-driven technologies such as adaptive learning platforms, recommendation systems, chatbots, and generative AI tools, which has normalized AI as part of their learning and social environments. This exposure contributes to a high level of ease and confidence when using digital platforms for communication, collaboration, research, and creative work. Many students now move fluidly between learning management systems, productivity apps, and online content creation tools, demonstrating digital fluency that supports both academic and personal tasks.

At the same time, the rapid expansion of AI across industries has sparked genuine curiosity among youth about future career opportunities in fields such as machine learning, data science, cybersecurity, and software development. Career-focused programs, extracurricular clubs, and media coverage of AI innovations further reinforce this interest, motivating students to explore STEM pathways and seek opportunities to build technical skills. Together, these trends suggest that Ontario's learners are not only comfortable with current digital tools but are also increasingly motivated to engage with the technologies shaping the future workforce

III. *Gaps*

Despite students' growing exposure to digital tools, significant gaps persist in their understanding of how artificial intelligence actually works and how to use it responsibly. Many learners hold misconceptions about AI's capabilities, often assuming that AI systems "*think*" like humans or possess perfect accuracy, which can lead to over-trusting automated outputs. These misconceptions make it harder for students to recognize AI-generated misinformation, especially as synthetic text, images, and videos become increasingly sophisticated and difficult to distinguish from authentic content [34].

In addition, students generally have limited awareness of algorithmic bias—how training data, model design, and systemic inequities can shape AI outputs in ways that reinforce stereotypes or exclude certain groups. This lack of understanding reduces their ability to critically evaluate AI-driven decisions or question the fairness of automated systems. Compounding these challenges is widespread uncertainty about the ethical use of generative AI in academic and personal contexts, including issues related to plagiarism, data privacy, transparency, and responsible attribution. Together, these gaps highlight the need for structured instruction that builds students' critical thinking, ethical reasoning, and technical understanding of AI.

IV. *Learning Needs*

From the perspective of the province of Ontario, the growing integration of artificial intelligence into education highlights an urgent need to provide students with clear and consistent guidelines for responsible AI use. While many learners are already experimenting with generative tools, adaptive platforms, and automated systems, their use is often shaped by informal habits rather than structured expectations.

Without province-wide guidance, students may struggle to understand when AI use is appropriate, how to acknowledge AI-assisted work, or how to protect their privacy when interacting with digital tools. Establishing clear, age-appropriate guidelines—embedded across subjects and grade levels—would help ensure that all Ontario students develop a shared understanding of academic integrity, data protection, and ethical digital behaviour. Such guidelines would also support teachers, who currently face wide variation in board-level policies and access to professional development.

Ontario students also need explicit instruction on how to evaluate AI-generated outputs, a skill that is becoming essential as generative systems produce increasingly convincing text, images, and data. Students must learn to question the accuracy, reliability, and potential biases embedded in AI outputs, rather than accepting them at face value. This includes understanding how training data shapes AI behaviour, recognizing the limitations of automated tools, and developing strategies for cross-checking information. Embedding these competencies into the curriculum would strengthen students' critical thinking and help them navigate a digital landscape where misinformation—much of it is AI-generated—is becoming more prevalent. Instruction of this kind aligns with Ontario's broader goals for media literacy and digital citizenship, but it requires intentional expansion to address the unique challenges posed by AI.

Finally, Ontario learners would benefit from opportunities to explore AI ethics and engage directly with transparent AI systems. Ethical considerations—such as fairness, accountability, privacy, and the societal impacts of automation—are central to preparing students for a future shaped by AI-driven decision-making. Providing structured opportunities to analyze real-world case studies, debate ethical dilemmas, and examine how AI systems make predictions would deepen students' understanding of both the promise and risks of emerging technologies.

Hands-on experiences with transparent or explainable AI tools would further demystify how algorithms function, allowing students to see how inputs, rules, and data influence outputs. Such experiential learning would not only build technical literacy but also empower students to participate thoughtfully in conversations about AI governance, workforce transformation, and digital rights—topics that are increasingly relevant across Ontario's economy and society.

V. *Equity and Access Considerations*

Ontario's diverse student population requires differentiated approaches. Factors influencing digital literacy include socioeconomic status, access to devices, language barriers, and geographic disparities between rural and urban communities [26].

Ensuring equitable access to AI and cybersecurity education is essential for reducing digital divides. Additional supports—such as targeted funding, culturally responsive resources, and multilingual digital learning tools—can help address these inequities. School boards also benefit from

partnerships with community organizations and industry to expand access to technology and specialized learning opportunities. By prioritizing inclusive strategies, Ontario can ensure that all learners develop the competencies needed to participate fully and safely in an increasingly digital world.

IMPLICATIONS FOR CURRICULUM AND INSTRUCTIONS

I. *Curriculum Integration*

AI and cybersecurity literacy can be embedded across subject areas, including science, mathematics, social studies, media literacy, and computer studies. Integrating AI and cybersecurity literacy across Ontario's curriculum offers a powerful way to ensure that all students—regardless of grade level or program pathway—develop the knowledge and critical thinking skills needed to navigate an increasingly digital world. Embedding these competencies into *science* allows students to explore how algorithms, data, and automation shape scientific discovery, while also examining the ethical implications of technologies such as *machine learning* in fields like health, climate science, and biotechnology.

In *mathematics*, students can deepen their understanding of data literacy by working with real-world datasets, analyzing patterns, and learning how statistical bias influences AI outputs, helping them see the connection between mathematical reasoning and algorithmic decision-making. Within *social studies*, AI and cybersecurity concepts can be linked to citizenship, governance, and global issues, enabling students to investigate topics such as digital rights, surveillance, misinformation, and the societal impacts of automation on work and equity. *Media literacy* provides a natural space to teach students how to evaluate AI-generated content, recognize deepfakes, understand how recommendation systems shape online experiences, and critically assess the credibility of digital information. Finally, *computer studies* can offer hands-on opportunities for students to experiment with transparent AI models, practice secure coding habits, explore cybersecurity tools, and understand the technical foundations of encryption, authentication, and threat detection.

By weaving AI and cybersecurity literacy throughout these subject areas, Ontario can create a cohesive, future-ready curriculum that equips students with both the practical skills and ethical awareness needed to thrive in a rapidly evolving technological landscape

II. *Teachers' Training*

Educators are the central drivers of any meaningful shift in AI, digital literacy, and cybersecurity education, making their capacity and confidence essential for successful implementation. To meet emerging classroom demands, teachers require sustained professional development on AI tools, cybersecurity best practices, and effective assessment strategies. Research consistently shows that without targeted training; educators struggle to translate complex technological concepts into age-appropriate learning experiences. Professional learning must therefore include hands-on exploration, ethical considerations, and opportunities to practice evaluating digital risks. Building this capacity not only strengthens instructional quality but also ensures that students receive accurate, relevant, and safe guidance in an increasingly digital world.

Strengthening teacher training is essential for Ontario to build a future-ready education system, as educators need sustained, high-quality professional development on AI tools, cybersecurity best practices, and effective assessment strategies to confidently guide students in a rapidly evolving digital landscape. Many teachers are already integrating digital platforms into their instruction, but the emergence of generative AI, algorithmic decision-making, and increasingly sophisticated cyber threats requires a deeper level of technical and pedagogical expertise.

Professional development must extend beyond basic tool use to help educators understand how AI systems function, evaluate their limitations, and model responsible, ethical use. In cybersecurity, teachers need training in secure practices, threat identification, data protection, and incident response so they can safeguard their environments and teach students to protect themselves. Assessment strategies must also help educators distinguish authentic learning from AI-assisted work, design tasks that promote critical thinking, and establish transparent guidelines for acceptable AI use. Comprehensive, ongoing professional learning ensures educators can use emerging technologies effectively while cultivating the AI, digital, and cybersecurity competencies students need to thrive.

III. *System Level Policy*

School boards should develop responsible AI use policies, cybersecurity protocols, and data privacy standards. At the system level, Ontario school boards play a critical role in creating the structural conditions necessary for safe, ethical, and future-ready technology use, making it essential for them to develop comprehensive policies on responsible AI use, cybersecurity, and data privacy.

Ontario school boards need clear AI-use policies, academic integrity guidelines, and transparent oversight. Strong cybersecurity protocols—covering threat prevention, incident response, staff training, and secure networks—are essential as phishing and ransomware risks grow. Without standardized procedures, responses vary and vulnerabilities increase. Consistent data-privacy standards and a coordinated system-wide approach ensure safer digital learning and confident technology integration.

RECOMMENDATIONS

I. *For Educators*

A well-rounded digital learning strategy should combine structured AI and cybersecurity modules with hands-on, real-world scenarios that help students apply their knowledge in meaningful ways. Simulations and practical activities deepen understanding by mirroring the kinds of challenges

learners will face beyond the classroom. At the same time, teaching students to critically evaluate digital content strengthens their ability to navigate misinformation and AI-generated media. Reinforcing safe digital habits throughout this process ensures that students not only build technical skills but also develop the awareness needed to protect themselves in an increasingly complex online environment.

- Implement structured AI and cybersecurity modules
- Use real-world scenarios and simulations
- Teach critical evaluation of digital content
- Reinforce safe digital habits

II. *For School Boards*

For school boards, strengthening digital learning begins with providing centralized resources and comprehensive teacher training so educators feel confident integrating new technologies into their classrooms. Establishing consistent policies across schools helps ensure that students receive equitable instruction and that digital practices align with provincial expectations. By partnering with cybersecurity and AI experts, boards can bring specialized knowledge into curriculum planning, enhance professional development, and ensure that students are learning skills that reflect real-world challenges and industry standards.

- Provide centralized resources and teacher training
- Develop consistent policies across schools
- Partner with cybersecurity and AI experts

III. *For Ministry of Education, Ontario*

For the Ontario Ministry of Education, strengthening the province's digital future begins with formally integrating AI and cybersecurity literacy into curriculum expectations so that every student develops foundational skills. Sustained funding for digital literacy initiatives is essential to support school boards, educators, and community partners as they implement new learning opportunities. Ongoing research on student competencies will help the province understand emerging gaps and guide evidence-based policy decisions. Ensuring equitable access to technology across all regions—urban, suburban, and rural—will be critical to making these efforts inclusive and effective for every learner.

- Integrate AI and cybersecurity literacy into curriculum expectations
- Fund digital literacy initiatives
- Support ongoing research on student competencies
- Ensure equitable access to technology

CONCLUSION

AI and cybersecurity literacy are now foundational for preparing Ontario students to navigate learning, work, and civic life in a technology-driven society. While many learners feel confident using everyday digital tools, these abilities represent only surface-level proficiency. Students increasingly need deeper insight into how AI systems function, how data is collected and processed, and how algorithmic decisions influence the information they encounter. Cybersecurity literacy must also extend beyond basic password practices to include recognizing sophisticated threats, protecting personal data, and understanding how social engineering exploits human behavior. Without these competencies, students remain vulnerable to misinformation, privacy breaches, and digital manipulation despite appearing technologically skilled. Addressing these gaps requires structured, intentional learning from early grades through secondary school. This includes hands-on engagement with transparent AI tools, ethical discussions embedded across subject areas, and practical cybersecurity exercises grounded in real-world scenarios. Clear and consistent curriculum expectations are essential to ensure equitable access across Ontario. When students receive coherent instruction, they shift from passive technology users to critical thinkers who can question AI outputs, identify risks, and make informed decisions about their digital presence. Achieving this vision demands coordinated action across the education system. Curriculum updates must explicitly integrate AI concepts, data literacy, and cybersecurity practices. Teacher training must equip educators to model responsible technology use. School boards must maintain consistent policies on AI, privacy, and cybersecurity. Together, these efforts can support genuine digital empowerment, enabling students to become informed, ethical, and resilient participants in an evolving digital society.

REFERENCES

[1] Canadian Teachers' Federation. (2025). Artificial intelligence (AI) legislative and policy scan: Gaps and risks in K–12 education. Canadian Teachers' Federation.

[2] Hagerman, M. S., & Neisary, S. (2024). Digital literacies learning needs in rural Ontario elementary schools: Teacher insights. Canadian Journal of Education, 47(2), 522–554.

[3] Information and Privacy Commissioner of Ontario. (2024). *Digital privacy charter for Ontario schools*. IPC Ontario. Ontario Ministry of Education. (2023). *Digital learning strategy: Preparing students for a connected world*. Government of Ontario.

[4] Ontario School Boards' ICT Council. (2024). *Cybersecurity readiness in Ontario K–12 schools: A system-level review*. OSBIC.

[5] AI Ethics Lab. (2025). *AI literacy KSAM method*. Rutgers University. https://aiethicslab.rutgers.edu/glossary/ai-literacy-ksam-method/

[6] Long, D., Magerko, B., & Nourbakhsh, I. (2021). *AI literacy: The essential skill set for a future workforce*. Communications of the ACM, 64(11), 30–33.

[7] Ng, D. T. K., Leung, J. K. L., & Chu, S. K. W. (2021). *Developing AI literacy in K–12 education: A systematic review*. Journal of Educational Computing Research, 59(7), 1312–1345.

[8] Touretzky, D. S., Gardner-McCune, C., Martin, F., & Seehorn, D. (2019). *Envisioning AI for K–12: What should every child know about AI?* AI Magazine, 40(4), 92–101.

[9] Williams, R., & Lombrozo, T. (2023). *Teaching students to reason about AI systems: Challenges and opportunities*. Learning, Media and Technology, 48(2), 145–162.

[10] Canadian Centre for Cyber Security. (2023). *National cyber security awareness strategy: Building a cyber-resilient Canada*. Government of Canada.

[11] KnowledgeFlow Cybersafety Foundation. (2025). *K–12 cybersafety curriculum: Integrating AI safety and ethical use*. KnowledgeFlow.

[12] Parkin, S., & Renaud, K. (2020). *Developing cybersecurity education for young learners: A framework for schools*. Computers & Security, 92, 101739.

[13] Alshaikh, M. (2020). *Developing cybersecurity awareness in K–12 education: A systematic review*. Computers & Education, 158, 103983.

[14] Ottawa Catholic School Board. (2025). *Digital literacy and cyber awareness: A whole-school approach*. OCSB.

[15] UNESCO. (2024). *User empowerment through media and information literacy responses to the evolution of generative artificial intelligence*. UNESCO IITE.

[16] Ontario Association of Media Literacy. (2023). *Media literacy in the age of AI: A guide for Ontario educators*. OAML.

[17] Hobbs, R. (2021). *Media literacy and the rise of generative AI: Implications for education*. Journal of Media Literacy Education, 13(2), 1–15.

[18] Livingstone, S., & Byrne, J. (2020). *Youth digital literacy: Understanding online risks and opportunities*. Journal of Children and Media, 14(2), 165–181.

[19] Mihailidis, P. (2018). *Civic media literacies: Re-imagining engagement for a digital age*. Routledge.

[20] van Dijk, J. (2020). *The digital divide: Understanding inequalities in digital skills and access*. Polity Press.

[21] Warschauer, M., & Matuchniak, T. (2010). *New technology and digital worlds: Analyzing evidence of equity in access, use, and outcomes*. Review of Research in Education, 34(1), 179–225.

[22] Haight, M., Quan-Haase, A., & Corbett, B. A. (2014). *Revisiting the digital divide in Canada: The impact of demographic factors on access to the internet*. Information, Communication & Society, 17(4), 503–519.

[23] People for Education. (2023). *Digital learning in Ontario: Equity, access, and student experience*. People for Education.

[24] eCampusOntario. (2022). *Digital fluency framework: Preparing learners for a technology-rich future*. eCampusOntario.

[25] McMahon, R., McNally, M. B., Nitschke, E., Napier, K., Alvarez Malvido, M., & Akçayir, M. (2024). Codesigning community networking literacies with rural/remote Northern Indigenous communities in Northwest Territories, Canada. *Journal of Computer-Mediated Communication, 29*(1), zmad042.

[26] eCampusOntario. (n.d.). *About eCampusOntario*. https://www.ecampusontario.ca

[27] Johnson, N. (2024). *Pan-Canadian report on digital learning*. Canadian Digital Learning Research Association (CDLRA).

[28] Johnson, N. (2025). *2025 Pan-Canadian report on digital learning trends*. Canadian Digital Learning Research Association (CDLRA).

[29] Higher Education Quality Council of Ontario. (2023). *Adopting a learning outcomes approach for digital literacy in Ontario postsecondary education*. HEQCO.

[30] Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security, 31*(8), 983–988.

[31] Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Influence techniques in phishing attacks: An empirical investigation. *Journal of Management Information Systems, 31*(1), 273–304.

[32] Canadian Commission for UNESCO. (2023). *AI competency framework for K–12 education*. UNESCO.

[33] Long, D., Magerko, B., & McKlin, T. (2021). AI literacy: A conceptual framework and systematic review. *International Journal of Artificial Intelligence in Education, 31*(4), 833–861.