1NC

Quarterfinals

Acton Boxborough ShNa vs. Lincoln Sudbury YS

For the past decade, we've been captivated by the vision of a future where gen AI opens up limitless possibilities. In truth, however, the AI sector is predominantly backed by corporations that fund research to create the illusion of success.

Ben Williamson, of the University of Edinburgh concludes in 2024(Ben Williamson is a Chancellor's Fellow at the Centre for Research in Digital Education and the Edinburgh Futures Institute at the University of Edinburgh. Alex Molnar is a Research Professor at the University of Colorado Boulder. Faith Boninger is NEPC's Publications Manager and Co-Director of NEPC's Commercialism in Education Research Unit and holds a PhD from Ohio State University. Williamson, B. Molnar, A., & Boninger, F. (2024). "Time for a pause: Without effective public oversight, AI in schools will do more harm than good." Boulder, CO: National Education Policy Center. http://nepc.colorado.edu/publication/ai) //Bellaire MC

Existing and potential uses of AI in education are not merely innovative technical add-ons to teaching and learning practices or engineering solutions to schools' existing pedagogic and administrative problems. Rather, AI in education has been spurred by multiple forces: longstanding efforts by scientists to measure, predict, and support learning processes and outcomes; commercial aspirations to profit from selling products to schools; and the political objective of being perceived as having improved school efficiency and accountability while cutting costs. As things currently stand, these ambitions have begun to coalesce into a vision of AI-driven schooling in which commercial products assess student learning, automate teaching, and make decisions about student progress. Inadequate Research Base¶ Despite the extensive research in the field of AI in Education (AIED) and the burgeoning¶ research on machine learning, there is **remarkably little** evidence to support claims of AI's ability to "transform" schools.76 While AIED researchers have produced many research findings, their studies tend to focus primarily on measures of individual student engagement and performance (assessed by standardized achievements tests), or on "engineering" problems such as designing increasingly sophisticated algorithms and enhancing machine learning effectiveness.77¶ Overall, AIED studies tend to find ambiguous results, lack independence and scale, and fail to address more fundamental questions **about educational goals**.78 AIED research therefore often promotes a view of education transformation as improving measurable individual outcomes despite very limited evidence that AI "works."79 In effect, such studies reduce well-researched and nuanced theories of how humans learn to whatever can be made into a mathematical model (however complex), and they ignore the contested terrain of exactly which goals and curriculum public schools should embrace.80 Moreover, **claims that AI can** solve major educational problems—such as lack of qualified teachers, student underachievement, and educational inequalities—rely to a considerable extent on **conjecture rather than evidence.**81¶ Even more problematic are the serious methodological flaws in machine learning research that call into question the validity of hundreds of studies.82 The nature of the flaws, in general, leads toward "over optimism" with respect to the usefulness and value of machine learning applications in a variety of fields.83 These findings are particularly concerning because they call into question not only commercial marketing claims, but also the scientific evidence base supporting the widespread implementation of AI systems in all sectors,84 including education. Finally, because of the very high computing costs associated with running machine learning models, most researchers have to rely on systems from the dominant AI companies themselves in order to conduct research85—the same corporations that often fund AI studies.86 This makes research dependent on corporate resources, funds, and business practices, giving AI firms considerable influence over not only AI development, but also the academic research that depends on their systems.87 It also compromises an important part of the research process, which is reproducing findings to verify their validity. When a company changes or stops supporting a particular model, researchers cannot reproduce studies conducted earlier.88 This renders the research base unstable and unverifiable—and thus unusable as a basis for assessing subsequent models.

Thus, to stabilize a future bent on the fallacies of AI, Acton is proud to negate.

Our First argument concerns Privacy.

Currently, efforts to regulate privacy risks of AI fail

Grosso et. Al 24 [Michelle R. Bowling & David P. Grosso, 02-21-2024, "The Development of AI and Protecting Student Data Privacy," ArentFox Schiff, https://www.afslaw.com/perspectives/ai-law-blog/the-development-ai-and-protecting-student-data-privacy] shake

Current Children's Privacy Landscape While **there are not laws that directly govern** the **intersection of AI and education**, several laws and regulations indirectly touch upon this area, specifically in regulating data privacy. Notably, President Joe Biden's Executive Order from October 30, 2023, lays out a comprehensive strategy for the development and deployment of AI, which includes strict safety and security standards, a focus on privacy protection, and countermeasures against potential AI-induced discrimination. The order promotes the responsible use of AI in various sectors, including education and healthcare, and emphasizes international collaboration on AI matters. As for current laws that indirectly regulate this area, federal regulations do offer some protections for pre-K to 12th grade students. The Children's Online Privacy Protection Act (**COPPA**) sets specific requirements for operators of websites or online services that knowingly collect personal data from children under 13. These operators must notify parents and secure their explicit consent before collecting, using, or disclosing a child's personal information. They must also ensure the safety of the collected information. However, a loophole allows schools to consent on behalf of parents if the education technology service provides the school with COPPA-mandated data collection notices and practices. The FTC proposed codifying this loophole in a Notice of Proposed Rulemaking released on December 20, 2023. Other than a slight change in the proposed rule from the prior guidance, which is a new exception that allows parents to review collected data, refuse to permit operators' further use or future online collection of personal information, and to direct operators to delete such information, schools can continue to consent on behalf of students. Furthermore, COPPA falls short as it doesn't extend to teenagers and most websites don't verify users' ages, often leading to websites unknowingly interacting with minors. The inability to reliably obtain parental consent online presents another challenge. As a result, websites that comply with COPPA often resort to expensive offline verification methods or, in the worst-case scenario, disregard the regulation altogether. Similarly, the Family Education Rights and Privacy Act (FERPA) was enacted to protect the privacy of student education records. It gives parents and students the right to access, amend, and control the disclosure of their education records. However, like COPPA, there are limitations. Private schools that do not receive funds are not protected under FERPA. FERPA does not prohibit the disclosure of directory information, such as the student's name, address, and phone number unless the student or parent has opted out of such disclosure. Likewise, the Protection of Pupil Rights Act (PPRA) provides certain rights for parents of students such as student participation in surveys and use of personal information for marketing purposes. PPRA only applies to programs and activities funded by the US Department of Education (ED). does not apply to the rights of students who are 18 years old or emancipated minors, and fails to address all aspects of student privacy such as the use of biometric data, online tracking, or data security.

This lack of regulation is dangerous because data breaches are surging.

Viano 24 [Andy Viano, 06-12-2024, "Cyberattacks on Higher Ed Rose Dramatically Last Year, Report Shows," Technology Solutions That Drive Education, https://edtechmagazine.com/higher/article/2024/03/cyberattacks-higher-ed-rose-dramatically-last-year-report-shows] shake

Higher **education institutions** were once again **inundated by cyberattacks** in 2023, according to a report from Malwarebytes, which called it **"the worst ransomware year on record" for the education sector.** The grim statistics include a **105 percent increase in** known ransomware **attacks against K–12 and higher education**, surging **from** 129 in 2022 to 265 **last year**. In higher education specifically, attacks were up 70 percent (68 in 2022 to 116 in 2023). Those numbers are based only on incidents in which a ransom was not paid, the report notes, meaning that the **actual number of attacks** was **probably significantly higher**.

And, its only going to get worse — Experts agree

Gartney 25 [Our expert guidance and tools enable faster, smarter decisions and stronger performance on an organization's mission-critical priorities.] 2-17-2025, "Gartner Predicts 40% of AI Data Breaches Will Arise from Cross-Border GenAI Misuse by 2027", Gartner, https://www.gartner.com/en/newsroom/press-releases/2025-02-17-gartner-predicts-forty-percent-of-ai-data-breaches-will-arise-from-cross-border-genai-misuse-by-2027] shake

By 2027, more than 40% of AI-related **data breaches** will be **caused by** the **improper use of generative AI** (GenAI) across borders, according to Gartner, Inc. The swift **adoption of GenAI technologies** by end-users has **outpaced** the **development of** data governance **and security measures**, raising concerns about data localization due to the centralized computing power required to support these technologies. "Unintended cross-border data transfers often occur due to insufficient oversight, particularly when GenAI is integrated in existing products without clear descriptions or announcement," said Joerg Fritsch, VP analyst at Gartner. "Organizations are noticing changes in the content produced by employees using GenAI tools. While these tools can be used for approved business applications, they pose security risks if sensitive prompts are sent to AI tools and APIs hosted in unknown locations." Global AI Standardization Gaps Drives Operational Inefficiency The lack of consistent global best practices and standards for AI and data governance exacerbates challenges by causing market fragmentation and forcing enterprises to develop region-specific strategies. This can limit their ability to scale operations globally and benefit from AI products and services. "The complexity of managing data flows and maintaining quality due to localized AI policies can lead to operational inefficiencies," said Fritsch. "Organizations must invest in advanced AI governance and security to protect sensitive data and ensure compliance. This need will likely drive growth in AI security, governance, and compliance services markets, as well as technology solutions that enhance transparency and control over AI processes."

Unfortunately, AI risks the privacy and data of students

Nambiar 24 [Nambiar, Anjali. 2024. Securing Student Data in the Age of Generative AI, raise.mit.edu/wp-content/uploads/2024/06/Securing-Student-Data-in-the-Age-of-Generative-AI_MIT-RAISE.pdf. Accessed 28 Feb. 2025.] shake

In addition to all the **data privacy-related issues associated with** the usage of traditional technology platforms in the classroom, **Gen AI poses** a **great**er **vulnerability**. This is because **it involves many dynamics associated with data**, from **using it to train** the **model to thriving on user input and customizing the output based on** the **data** that **users input**. These **complex interactions** between such models and data **make data privacy even more challenging** to ensure in the case of AI applications. As per the study " Unveiling security, privacy, and ethical concerns of ChatGPT" specific challenges solely associated with Gen AI are as follows: **Privacy leakage due to personal input exploitation**: Imagine an **AI EdTech tool collects students' browsing history to personalize learning. If** this data is **shared with advertisers without consent, it breaches privacy**. Even if it's **stored insecurely and accessed by unauthorized parties**, it **poses risks**. **1,619** Additional privacy concerns due to **Gen AI** integration **cases of cyber attacks in schools** since 2016* *as per The K-12 Cyber Incident Map by K12 SIX To prevent such breaches, strict data protection measures and transparent data practices are essential. Emerging new privacy attacks on LLMs such as "Jailbreaking": In the context of Large Language Models (LLMs) like ChatGPT, **users could** potentially reverse engineer or "**Jailbreak**" **the system to access info**rmation **from previous conversations stored in its memory**. For instance, if someone manages to exploit a vulnerability in the LLM's security, they could **extract sensitive data from student users' interactions, compromising privacy.** This highlights the importance of robust security measures and encryption protocols to safeguard users' information in AI chat interfaces. A solution that helps ensure student data is not shared with third parties and helps students and other stakeholders be cautious of the data they enter into the application while interacting with it would be required to safeguard students' privacy against challenges unique to GenAI tools.

And, GenAI has limited oversight, leading to subpar code riddled with vulnerabilities

Roe 24 [Frank Roe, xx-xx-xxxx, "The Software Industry Is Facing an AI-Fueled Crisis. Here's How We Stop the Collapse.," Built In, https://builtin.com/artificial-intelligence/ai-fueled-software-crisis] shake

Enter generative AI. Hailed as a game-changer, generative AI has undeniably transformed software development, but it's important to remain aware of the potential complexities and risks it introduces. As **generative AI tools have** lowered the barrier to entry for code creation and democratized software development, the foundation of our software-dependent world has come under threat. **Limited oversight** has **le[ading] to an influx of subpar code, often riddled with bugs and vulnerabilities** that enter the system. The increasingly common practice of having non-technical individuals create code exacerbates the issue because they may not understand the intricate nuances and potential downstream consequences of the code they're creating. The lack of understanding about coding complexities and the necessity of rigorous testing is leading to a degeneration in code quality. This trend is evidenced by increasing reports of software failures, which are often linked to overlooked coding errors and inadequate testing. Studies have shown that as more people with limited programming experience contribute to codebases, the number of critical bugs and security vulnerabilities undergoes a significant increase. For example, **Synopsys' 2024 Open Source Security and Risk Analysis** report highlights that nearly **three-quarters of commercial codebases contain high-risk, open-source vulnerabilities with** a sharp increase in these vulnerabilities attributable to the involvement of **less experienced contributors.**

In a holistic study by Microsoft and Carnegie Melon, researchers find

Merod 25 [Anna Merod, "PowerSchool data breach brings claims of negligence, poor cyber hygiene", 01/22/2025, Cybersecurity Dive, https://www.cybersecuritydive.com/news/powerschool-data-breach-lawsuits-negligence/737961/, Accessed 03/29/2025] [shivank]

Since **PowerSchool revealed earlier this month that it had fallen victim to a data breach**, many questions remain about the impact and implications for student and staff data in school districts that use PowerSchool's software nationwide. PowerSchool is expected to release a report soon based on findings from CrowdStrike, a cybersecurity company investigating the situation. Information from that report will be shared directly with PowerSchool customers, a company spokesperson told K-12 Dive in an email Friday. The K-12 software company told K-12 Dive earlier this month that it became aware on Dec. 28 of what it called a "potential" cybersecurity incident in which a threat actor gained unauthorized access to an unknown amount of student and staff data from its PowerSource service. PowerSource is a customer support portal for district and school staff. The threat actor is believed to have stolen data from two tables containing family and teacher information from PowerSchool's Student Information System database. **Some of that data may include personally identifiable information like names and addresses of families and educators. In some cases, information such as Social Security numbers and medical data were also exposed. A lack of cyber hygiene? While PowerSchool told K-12 Dive the incident was not a ransomware attack, a news report from Bleeping Computer said the software company's FAQ page for customers acknowledged that it paid the threat actor following the data breach**. When K-12 Dive previously asked PowerSchool if the company had paid the threat actor, a spokesperson said: "We have taken all appropriate steps to prevent the data involved from further unauthorized misuse. The incident is contained and we do not anticipate the data being shared or made public." In a Jan. 15 webinar, national school cybersecurity nonprofit K12 Security Information eXchange invited cybersecurity experts to share reactions and next steps for school districts following the PowerSchool data breach. Doug Levin, co-founder and national director of K12 SIX, said during the webinar that any kind of payment to a threat actor via extortion imperils the education sector. Keep up with the story. Subscribe to the Cybersecurity Dive free daily newsletter Email:Sign up "It encourages malicious actors to continue to target us and try to extort us, either by using encryption to lock up our devices or stealing our data and trying to extort us to keep it from being leaked," Levin said. Levin added there's **no guarantee that any stolen data won't be further exploited and shared even if an organization pays a bad actor not to release it on the dark web. "I think it's certainly possible that it could show up there and be released at some point in the future, or it could be used to target individual teachers and students directly via phishing or social engineering," Levin said.** The FBI also strongly discourages victims of ransomware attacks from paying hackers for reasons similar to those Levin shared. Speakers on the webinar also raised questions about whether PowerSchool used multifactor authentication for its PowerSource service before the data breach. While PowerSchool's internal systems use multifactor authentication, the infiltrated PowerSource system did not have multifactor authentication support, a company spokesperson told K-12 Dive on Friday. However, PowerSchool said that has since been addressed through its remediation plan. Wesley Lombardo, technology director at Tennessee's Maryville City Schools, told the webinar that there's no reason a single user should be able to access all student and teacher data from every available school district. PowerSchool's lack of cyberhygiene is "pretty concerning," he said. "I feel like there were failures kind of along the way of places where they could have maybe not have stopped that initial access, but definitely as soon as the exfiltration started, [there] should have been bells and whistles and all kinds of things kind of alerting that something was amiss," Lombardo said.

And, Data breaches are problematic to schools…

Sutton 23 [Chelsea Sutton, 10-16-2023, "What is the cost of a data breach?," Office of Information Technology, https://oit.ncsu.edu/2023/10/16/what-is-the-cost-of-a-data-breach/] shake

According to IBM's 2023 Cost of a Data Breach Report, **the average cost of a data breach in** the higher **education** and training sector **was $3.65 million** between March 2022 and March 2023. **The mean time** for all sector**s to identify a data breach was 204 days with an additional 73 days on average to contain it**.

Merod 25 [Anna Merod, "PowerSchool data breach brings claims of negligence, poor cyber hygiene", 01/22/2025, Cybersecurity Dive, https://www.cybersecuritydive.com/news/powerschool-data-breach-lawsuits-negligence/737961/, Accessed 03/29/2025] [shivank]

Since **PowerSchool revealed earlier this month that it had fallen victim to a data breach**, many questions remain about the impact and implications for student and staff data in school districts that use PowerSchool's software nationwide. PowerSchool is expected to release a report soon based on findings from CrowdStrike, a cybersecurity company investigating the situation. Information from that report will be shared directly with PowerSchool customers, a company spokesperson told K-12 Dive in an email Friday. The K-12 software company told K-12 Dive earlier this month that it became aware on Dec. 28 of what it called a "potential" cybersecurity incident in which a threat actor gained unauthorized access to an unknown amount of student and staff data from its PowerSource service. PowerSource is a customer support portal for district and school staff. The threat actor is believed to have stolen data from two tables containing family and teacher information from PowerSchool's Student Information System database. **Some of that data may include personally identifiable information like names and addresses of families and educators. In some cases, information such as Social Security numbers and medical data were also exposed. A lack of cyber hygiene? While PowerSchool told K-12 Dive the incident was not a ransomware attack, a news report from Bleeping Computer said the software company's FAQ page for customers acknowledged that it paid the threat actor following the data breach**. When K-12 Dive previously asked PowerSchool if the company had paid the threat actor, a spokesperson said: "We have taken all appropriate steps to prevent the data involved from further unauthorized misuse. The incident is contained and we do not anticipate the data being shared or made public." In a Jan. 15 webinar, national school cybersecurity nonprofit K12 Security Information eXchange invited cybersecurity experts to share reactions and next steps for school districts following the PowerSchool data breach. Doug Levin, co-founder and national director of K12 SIX, said during the webinar that any kind of payment to a threat actor via extortion imperils the education sector. Keep up with the story. Subscribe to the Cybersecurity Dive free daily newsletter Email:Sign up "It encourages malicious actors to continue to target us and try to extort us, either by using encryption to lock up our devices or stealing our data and trying to extort us to keep it from being leaked," Levin said. Levin added there's **no guarantee that any stolen data won't be further exploited and shared even if an**

organization pays a bad actor not to release it on the dark web. "I think it's certainly possible that it could show up there and be released at some point in the future, or it could be used to target individual teachers and students directly via phishing or social engineering," Levin said. The FBI also strongly discourages victims of ransomware attacks from paying hackers for reasons similar to those Levin shared. Speakers on the webinar also raised questions about whether PowerSchool used multifactor authentication for its PowerSource service before the data breach. While PowerSchool's internal systems use multifactor authentication, the infiltrated PowerSource system did not have multifactor authentication support, a company spokesperson told K-12 Dive on Friday. However, PowerSchool said that has since been addressed through its remediation plan. Wesley Lombardo, technology director at Tennessee's Maryville City Schools, told the webinar that there's no reason a single user should be able to access all student and teacher data from every available school district. PowerSchool's lack of cyberhygiene is "pretty concerning," he said. "I feel like there were failures kind of along the way of places where they could have maybe not have stopped that initial access, but definitely as soon as the exfiltration started, [there] should have been bells and whistles and all kinds of things kind of alerting that something was amiss," Lombardo said.

C2 IS Critical thinking

AI is used heavily in education by students

Education Council 24 [Digital Education Council, "What Students Want: Key Results from DEC Global AI Student Survey 2024", August 7 2024, https://www.digitaleducationcouncil.com/post/what-students-want-key-results-from-dec-global-ai-student-survey-2024]

86% of students globally **are regularly using AI in their studies**, with **54% of them using AI on a weekly basis, the** recent **Digital Education Council Global AI Student Survey found. ChatGPT was found to be the most widely used AI tool, with 66% of students using it**, and over 2 in 3 students reported using AI for information searching. Despite their high rates of AI usage, 1 in 2 students do not feel AI ready. 58% reported that they do not feel that they had sufficient AI knowledge and skills, and 48% do not feel adequately prepared for an AI-enabled workplace. **The Digital Education Council survey was conducted in July 2024 and comprised responses from more than 3,800 students from 16 countries**. "The rise in AI usage forces institutions to see AI as core infrastructure rather than a tool" says Alessandro Di Lullo, CEO of the Digital Education Council and Academic Fellow in AI Governance at The University of Hong Kong. At the same time, "universities need to consider how to effectively boost AI literacy to equip both students and academics with the skills to succeed in an AI-driven world", he adds. Students have expectations and preferences for AI applications and integrations in their universities, but are dissatisfied with the current state of AI in universities, with 80% of students saying that AI in universities are not fully meeting expectations. Mr. Di Lullo said "given that only 5% of students indicated that they were fully aware of AI guidelines and feel that they are fully comprehensive - universities should swiftly respond to this dissatisfaction by improving AI guidelines and communicating them well. A starting point is the DEC AI Governance Framework that we published in June 2024."

AI kills critical thinking

Gerlich 25 [Michael Gerlich, "AI Tools in Society: Impacts on Cognitive Offloading and the Future of Critic", January 3 2025, Center for Strategic Corporate Foresight and Sustainability,, https://www.mdpi.com/2075-4698/15/1/6?utm_source=chatgpt.com]

This study investigated the impact of AI tool usage on critical thinking, considering cognitive offloading as a potential mediating factor. The analyses encompassed descriptive statistics, ANOVA, correlation analysis, multiple regression, and random forest regression. 4.1. Descriptive Statistics **The dataset comprised 666 responses detailing AI tool usage, cognitive offloading tendencies, and critical thinking scores**. **Younger participants** (17–25) **exhibited higher gen AI tool usage and cognitive offloading, but lower critical thinking scores**. **In contrast, older participants** (46 and above) **showed lower AI tool usage and cognitive offloading, with higher critical thinking scores**. Table 1 provides a summary of the dataset validation, including the number of valid and missing responses for each variable, as well as the range of numeric codes assigned to categorical variables, such as age, gender, and education level. This ensured that the dataset was complete and ready for further statistical analysis. Table 2 presents an overview of the categorical variables used in the study, including age, gender, education level, occupation, and deep thinking activities. Variable codes and detailed descriptions are available in Appendix A for reference. Table 1. Data validation summary. Table 2. Frequencies. 4.2. ANOVA The ANOVA results revealed significant differences in critical thinking scores across different levels of AI tool usage (p < 0.001), suggesting that higher AI tool usage is associated with reduced critical thinking abilities (Table 3). Additionally, to illustrate the relationship between demographic factors and cognitive engagement, we explored the impact of education level, age, and occupation on deep thinking activities. These analyses revealed significant effects of education level (p < 0.001), age (p < 0.001), and occupation (p < 0.001) on deep thinking activities (Table 4). The results indicate that higher education levels and older age groups are associated with greater engagement in deep thinking activities. Table 3. ANOVA results for critical thinking scores. Table 4. ANOVA results for deep thinking activities. Table 3 presents the ANOVA results **examining the relationship between levels of AI tool usage and critical thinking scores. The analysis revealed a highly significant effect (p < 0.001), indicating that increased reliance on AI tools is associated with reduced critical thinking abilities**. **These findings align with theories of cognitive offloading, where the automation of analytical tasks reduces the need for independent reasoning**.This underscores the need for strategies that balance the benefits of AI integration with the development of independent analytical skills, particularly in educational and organisational settings. Table 4 presents the ANOVA results examining the impact of demographic variables on deep thinking activities. Education level, age, and occupation were found to have significant effects, highlighting their critical roles in shaping cognitive engagement. Participants with advanced education levels and those in managerial roles exhibited higher levels of deep thinking, likely due to greater exposure to cognitively demanding tasks. Conversely, gender did not significantly influence deep thinking activities, suggesting that other factors may play a more prominent role. These findings underscore the interplay between demographic variables and cognitive engagement, offering actionable insights for educational and occupational strategies aimed at fostering critical thinking. In-depth analyses demonstrated significant differences in deep thinking activities across education level, age, and occupation. Post hoc comparisons indicated that individuals with advanced degrees and those in older age groups engaged in significantly more deep-thinking activities. These findings suggest that education and life experience play critical roles in fostering cognitive engagement. Given the ordinal nature of the 'deep thinking activities' variable, a Kruskal–Wallis test was performed to assess differences across education levels. This non-parametric test is particularly suited for comparing independent groups with ordinal data (Siegel and Castellan, 1988). The results revealed significant differences ($H(3) = 14.26$, $p < 0.01$), with higher education levels associated with greater scores for deep thinking activities. Post hoc pairwise comparisons using Dunn's test indicated significant differences between participants with a bachelor's degree and those with secondary education ($p < 0.01$), as well as between participants with a master's degree and those with secondary education ($p < 0.05$). These findings complement the ANOVA results by providing robust evidence that educational attainment plays a crucial role in fostering deeper cognitive engagement. 4.3. Correlation Analysis The correlation analysis highlighted strong negative correlations between AI tool usage and critical thinking variables (e.g., Evaluate_Sources: −0.494). Positive correlations were found between education level, deep thinking activities, and critical thinking scores (Table 5). Table 5. Correlation matrix. The correlation analysis (Table 5) revealed key relationships between the study's variables: AI Tool Use and Critical Thinking: There is a strong negative correlation, indicating that increased use of AI tools is associated with lower critical thinking skills. AI Tool Use and Cognitive Offloading: A strong positive correlation suggests that higher AI usage leads to greater cognitive offloading. Cognitive Offloading and Critical Thinking: Similarly, there is a strong negative correlation, showing that as cognitive offloading increases, critical thinking decreases. These patterns highlight the cognitive impact of AI tool usage, particularly how reliance on AI tools may reduce critical thinking by encouraging cognitive offloading. The relationships between the key variables, namely, AI Tool Use, Cognitive Offloading, and Critical Thinking, are summarised in Table 6. These correlations provide critical insights into how reliance on AI tools impacts cognitive processes and critical thinking abilities. Table 6. Summary of correlations. **The analysis revealed a strong positive correlation ($r = +0.72$) between AI tool use and cognitive offloading, indicating that increased reliance on AI tools is associated with a higher degree of cognitive offloading. This finding aligns with existing literature suggesting that AI tools reduce the cognitive burden by automating routine tasks, allowing users to delegate memory, attention, and decision-making processes to technological systems** [5,16]. However, this convenience comes at a cost, as it reduces the opportunity for individuals to engage in cognitively demanding tasks, potentially undermining cognitive engagement over time. **The correlation between AI tool use and critical thinking was found to be strongly negative ($r = -0.68$), suggesting that greater reliance on AI tools is associated with a decline in critical thinking skills.** **This outcome is consistent with the theory of cognitive offloading, where AI reduces the necessity for users to employ deep analytical reasoning and independent problem-solving. The diminished practice of these skills can result in a long-term erosion of critical thinking capabilities**, a finding supported by prior studies highlighting the risks of over-reliance on technology for decision-making and information evaluation [4,6]. A strong negative correlation ($r = -0.75$) between cognitive offloading and critical thinking further supports this interpretation. As individuals increasingly offload cognitive tasks to AI tools, their ability to critically evaluate information, discern biases, and engage in reflective reasoning diminishes. This relationship underscores the dual-edged nature of AI technology: while it enhances efficiency and convenience, it inadvertently fosters dependence, which can compromise critical thinking skills over time.

Critical Thinking is the most important part of education
Siegel 08 [Harvey Siegel, "Critical Thinking as an Educational Ideal", January 30 2008, The Educational Forum, https://www.tandfonline.com/doi/pdf/10.1080/00131728009336046]

Many philosophers of education take critical thinking to be a central ideal of educational endeavor. **Scheffler**, for example, **holds that "critical thought is of the first importance in the conception and organization of educational activities**." **Popper takes critical thinking to be** not only a fundamental educational ideal, but **the very hallmark of serious intellectual activity (especially scientific activit**y): "criticism and critical discussion are our only means of getting nearer to the truth." If these thinkers applaud the notion of critical thought, however, there are also those, for example Kuhn, whose work suggests that critical thought is not all its proponents claim for it. What we are to make of this morass of contradictory views is not clear; however, the centrality of the notion of critical thought as an educational ideal necessitates serious treatment of the problem. What is the status of the ideal of critical thinking? This is the question addressed in the present article. In what follows I shall try, first, to say just what critical thinking is; what the ideal comes to. Then, I will examine the justifiability of critical thinking: given a clear account of the notion, on what grounds (if any) can critical thinking be defended as an educational ideal? This will lead to a consideration of one conspicuous argument against the ideal of critical thought—namely, that it is to be rejected on political grounds, as an ideal which cannot be justified on nonpolitical grounds and which masks unacceptable political assumptions.

Education without critical thinking is useless
North Whitehead 29 [Alfred North Whitehead, "The Aims of Education", 1929, New York Free Press, https://www.educationevolving.org/files/Whitehead-AimsOfEducation.pdf]

Culture is activity of thought, and receptiveness to beauty and humane feeling. Scraps of information have nothing to do with it. A merely well-informed man is the most useless bore on God's earth. What we should aim at producing is men who possess both culture and expert knowledge in some special direction. Their expert knowledge will give them the ground to start from, and their culture will lead them as deep as philosophy and as high as art. We have to remember that the valuable intellectual development is self development, and that it mostly takes place between the ages of sixteen and thirty. As to training, the most important part is given by mothers before the age of twelve. A saying due to Archbishop Temple illustrates my meaning. Surprise was expressed at the success in after-life of a man, who as a boy at Rugby had been somewhat undistinguished. He answered, "It is not what they are at eighteen, it is what they become afterwards that matters." In training a child to activity of thought, above all things we must beware of what I will call **"inert ideas"** -- **that is to say, ideas that are merely received into the mind without being** utilised, or tested, or **thrown into fresh combinations**. In the history of education, the most striking phenomenon is that schools of learning, which at one epoch are alive with a ferment of genius, in a succeeding generation exhibit merely pedantry and routine. The reason is, that they are overladen with inert ideas. **Education with inert ideas is ot only useless: it is, above all things, harmful** -- Corruptio optimi, pessima. Except at rare intervals of intellectual ferment, education in the past has been radically infected with inert ideas. That is the reason why uneducated clever women, who have seen much of the world, are in middle life so much the most cultured part of the community. They have been saved from this horrible burden of inert ideas. Every intellectual revolution which has ever stirred humanity into greatness has been a passionate protest against inert ideas. Then, alas, with pathetic ignorance of human psychology, it has proceeded by some educational scheme to bind humanity afresh with inert ideas of its own fashioning

2NC

On language barrier

Analytics

On personalized learning

1. [ID] AI systems actually increase disparities due to bias.

DigitalDefynd 25 [Team DigitalDefynd, (No quals) "Rise of AI Tutors: Can They Replace Human Teachers? [2025]", January 2025, digitaldefynd, https://digitaldefynd.com/IQ/rise-of-ai-tutors/#:~:text=AI%2Ddriven%20learning%20tools%20depend,rather%20than%20closing%20learning%20gaps.] // xer

AI-driven learning tools depend on the quality of the **data they are trained with** and **if that data contains biases, it can** result in inequitable educational outcomes. If an AI tutor is trained on skewed or incomplete data, it may **reinforce existing educational disparities rather than closing learning gaps.**

Mostly analytics