

大语言模型赋能高校安全教育的路径研究

刘艳新

广州航海学院, 广东 广州 510725

DOI:10.61369/ASDS.2025090011

摘要： 本文从大语言模型视角探讨其在高校安全教育中的赋能路径。研究表明，大语言模型可实现安全教育内容的动态生成、知识获取的个性化及学习体验的交互式提升，但也面临价值引导与数据安全等挑战。据此，本文构建了创新框架，从智能内容供给、交互认知支持和数据安全治理三方面提出实践路径，为安全教育现代化转型提供参考。

关键词： 大语言模型；安全教育；大学生；人工智能；教育创新

A Study on the Pathways of Large Language Models Empowering College Safety Education

Liu Yanxin

Guangzhou Maritime University, Guangzhou, Guangdong 510725

Abstract： This paper explores the enabling pathways of large language models (LLMs) in university safety education from their perspective. Research shows that LLMs can facilitate the dynamic generation of safety education content, personalize knowledge acquisition, and enhance interactive learning experiences. However, they also face challenges such as value alignment and data security. Accordingly, this paper constructs an innovative framework and proposes practical approaches from three aspects: intelligent content provision, interactive cognitive support, and data security governance, offering insights for the modern transformation of safety education.

Keywords： large language model; security education; college students; artificial intelligence; educational innovation

引言

在全球化、信息化与智能化深度融合的时代背景下，高校大学生面临的安全问题日益多元复杂，其范围涵盖心理健康、网络安全、法律意识、防诈骗、防侵害等多个领域。安全稳定的校园环境是大学生身心健康和全面发展的重要基础。然而，当前高校安全教育在教学内容、方式和效果等方面仍存在不足：内容陈旧单一、形式呆板，教学以灌输为主，忽视学生的主体性与个性化需求，导致教育实效不强。

随着人工智能的快速发展，尤其是大语言模型（Large Language Model, LLM）的出现，为高校安全教育理念与模式创新提供了前所未有的机遇。大语言模型具备强大的语言理解、内容生成和交互对话能力，能够根据学生需求提供个性化的学习建议并自动生成教学资源，支持安全教育内容的动态更新与交互式学习体验的提升。

目前，学界对大学生安全教育的研究呈现多维度探索态势，如从思政融合^[1]、法治教育^[2]、心理健康^[3]、课程创新^[4]、信息安全^[5]等视角对大学生安全教育进行了探索，但在具体智能技术工具的教学应用与系统化创新路径方面仍显不足。随着大语言模型技术的迅速发展及其在知识生成、语义理解、智能交互等方面展现的优势，如何科学嵌入大语言模型构建智能化、个性化的大学生安全教育新范式已成为亟待研究的课题。基于此，本文以大语言模型赋能高校安全教育为切入点，探讨其教育赋能的实现路径与机制，旨在为高校安全教育的数字化转型提供理论依据和实践参考。

一、高校安全教育研究综述

这一重要论述深刻揭示了国家安全教育在维护国家安全体系中的基础性地位，为高校推进国家安全教育工作提供了根本遵循和方向指引。基于此，学术界从多个视角对大学生安全教育展开了广

习近平总书记指出：“要加强对人民群众的国家安全教育^[6]”，

基金项目：广州市哲学社会科学“十四五”规划项目（2021GZSZ19）、教育部人文社会科学研究专项任务项目（高校辅导员研究）（22JDSZ3091）。

作者简介：刘艳新（1980-），讲师，广州航海学院学工部副部长，硕士，研究方向：国家安全教育、思想政治工作。

泛研究与实践探索。例如，一是在思政与德育的融合视角上，李典和李阳^[7]从教育与管理协同视角探索安全管理策略，提升大学生安全素养与风险应对能力，保障校园稳定运行，为大学生学习生活成长提供良好的安全氛围。倪皓^[8]提出从法治视角入手，着力增强大学生的法治观念，培养大学生的自我保护能力，让大学生掌握更多的安全知识，已成为新时代高校必须正视并解决的重要问题。周光玲和黄义^[9]提出高校应提升教师数智素养、强化人文内核、完善数据责任体系，探索大模型赋能思政课创新路径。二是在心理健康与安全行为方面，陈启等^[10]提出使用大语言模型（Large Language Models, LLMs）生成心理健康支持回复，有助于减轻心理咨询师的负担，提高心理健康支持的效率。张丽园等^[11]提出披露主题的加入有助于问答模型有效学习并预测合适的支持策略，在线心理健康支持回答的生成效果得到显著提升。杨莹^[12]提出通过加强心理健康教育，引导学生正确面对压力，提升自我认知和情绪管理能力，对于增强他们的安全意识和行为至关重要。Dolan 和 Matsuno^[13]探讨了非二元大学生如何根据自己的身份来评估自己的安全，并对他们在校园中的性别歧视经历进行了意义建构。三是在教学模式与课程设计创新上，李红霞等^[14]以国家级一流本科课程“大学生国家安全教育”为例，优化教学方案设计构建全链条教学模式闭环，实现学生在知识获取中的效能感。高远民等^[15]提出安全教育实验室增加安全教育的实践性与广泛性，突出学员主体性和教学规范性，提高师生的实践素养和安全意识。North et al.^[16]分析了调查和访谈的数据，并制定了一个安全责任范围的框架：学生安全、立法要求、员工能力和文书工作。四是技术赋能与信息安全意识上，张树启^[17]提出要深耕课堂教学、调查研究、加强自我教育，构建管理、反馈、评价、保障四项网络安全教育机制。杨鉴炜^[18]提出借助人工智能不仅可以提高课程理论教学的针对性，还可以丰富课程实践教学形式。杜蕾和何斐^[19]提出高校信息素养教育应重信息辨识与批判思维、强信息安全与道德培养，提升学生素养适应数智时代。Mia et al.^[20]研究采用质性研究中的现象学研究方法，呈现了不同教育角色在实施数字监控应用程序（MA）以保护 k-12 学生免受伤害方面的经历并讨论了 MA 使用的影响，未来的需求，以及对学生的持续保护和监督。

综上，现有研究多聚焦思政融合、心理健康、教学创新与技术赋能等方面，但在具体技术工具的教学应用与系统化路径探索方面仍显不足。随着大语言模型技术的迅速发展，其在知识生成、语义理解与智能交互等方面的优势，为高校安全教育的内容创新与模式变革提供了新的可能。如何科学嵌入大语言模型，构建智能化、个性化的安全教育新范式，成为当前亟待探索的课题。基于此，本文以“大语言模型赋能高校安全教育的路径研究”为题，旨在探讨其教育赋能逻辑与应用路径，为高校安全教育的数字化转型提供理论与实践参考。

二、大语言模型赋能高校安全教育的创新路径

在高校大学生安全教育领域，大语言模型的引入不仅是一项

技术手段的革新，更是一种教育理念与教学机制的重塑。在已有研究成果^[21-25]的基础上，分析大语言模型在高校教育中的嵌入逻辑与技术特性，可以将其赋能路径归纳为以下三个维度：

（一）智能内容供给：实现资源动态生成与精准配置

1. 多源数据融合，增强内容的现实关联性。大语言模型具备从不同语境中提取、整合信息的能力，可将政策文献、校园案例、新闻事件等多元信息汇编成教学资源。如基于近期校园诈骗事件，模型可自动生成案例解析、行为预警提示与防范措施，实现教学内容的时效性与贴近性。

2. 场景化内容生成，提升学生代入感。大语言模型可根据设定情境模拟危险场景（如寝室火灾、网络约会陷阱、突发校园冲突等），形成沉浸式案例材料，学生在情境中进行判断与决策，有助于锻炼其安全感知能力与应变策略。

3. 教材辅助与自动化测评。通过对课程大纲和知识点的解析，大语言模型可辅助教师快速生成思政导语、安全警示语、测试题库与评分标准，提升教学效率与评估精度，构建“内容生成—教学实施—效果评价”闭环。

（二）交互认知支持：构建个性化、情境化的学习体验

1. 个性化交互反馈机制。学生可基于个体兴趣与困惑，自主提出问题，大语言模型根据其学习进度、表达风格提供多层次解答，如简明回答、概念解释或行为建议，提升学生的自主探索与理解深度。

2. 情境对话训练系统。结合校园实际，设计虚拟对话任务（如你接到陌生电话要求转账时该如何处理？），大语言模型以智能对话者身份与学生反复交互，模拟高风险沟通场景，提升其应对能力。

3. 学情跟踪与预警辅助。通过分析学生的提问频次、关键词与认知模式，大语言模型可初步识别可能存在的信息误区、情绪异常或行为偏差，为教师提供数据支持，及时开展干预与引导。

（三）数据安全治理：确保 AI 赋能过程中的教育伦理与隐私合规

在利用大语言模型赋能高校安全教育的过程中，数据安全与伦理治理是确保技术应用行稳致远的基石。它不仅是技术层面的防护，更是一项关乎法律遵从、伦理对齐与信任构建的系统性工程。为此，必须建立一个多层次、全方位的治理框架，将合规性、安全性与教育性融为一体。

1. 设立清晰的使用边界与严格的权限控制机制。高校作为数据控制者，必须首先在制度层面划清红线。应依据《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》等法律法规，制定专门的《校园 AI 应用数据安全管理条例》。该条例需明确界定不同教学场景下 LLM 的调用权限层级，例如，区分教师用于课程准备的内部调试权限与学生进行互动学习的受限访问权限。同时，必须严格规定敏感个人信息的存储周期、存储地点（如优先采用本地化部署）以及访问数据的审批流程，确保从数据入口到销毁的全生命周期都处于合法、合规、可控的状态，杜绝超范围采集和违规滥用。

2. 强化数据全生命周期的脱敏与匿名化处理。技术手段是保

障隐私的核心防线。在收集与处理学生输入的信息（如身份证）时，不能将原始数据直接馈送给模型。必须在数据预处理阶段执行严格的去标识化操作，系统性地删除或替换所有能直接或间接识别到学生个人身份的信息（如姓名、学号、手机号）。此后，应对处理后的数据采用强加密算法进行存储，确保即使发生数据泄露，攻击者也无法读取原始信息。更重要的是，需要建立技术屏障，防止模型在训练或推理过程中记忆并反推出个体身份。

3. 建立贴合教育场景的 AI 伦理审查与操作规范。安全教育的终极目标是“育人”，技术的应用绝不能偏离这一价值主线。因此，必须超越单纯的数据保护，制定一份面向高校安全教育场景的《AI 辅助教学伦理指南》。明确“人机协同”的边界，强调教师的主导地位不可替代。确保 AI 始终作为辅助工具，其输出能够符合社会主义核心价值观和学校的育人目标，维护教育的人文关怀与价值引导功能，避免出现技术依赖甚至价值导向偏差的风险。

三、结论与展望

（一）研究结论

本研究以大语言模型赋能高校大学生安全教育为核心议题，系统分析了其在教育内容生成、学习交互支持与数据安全治理等方面的创新路径。研究表明，大语言模型作为生成式人工智能的重要代表，其强大的语义理解与知识生成能力，为高校安全教育的数字化转型提供了新的理论支撑与技术工具。具体来说，首先，在智能内容供给方面，大语言模型通过对多源信息的整合

与语义再构，可实现教学资源的动态生成与精准匹配，打破传统安全教育内容更新滞后的局限，推动教学资源从静态呈现向动态生成转变。其次，在交互认知支持层面，大语言模型的人机对话特性重塑了学习过程的互动关系，通过个性化反馈、场景化训练与学习行为分析，促进学生从被动接受向主动建构转化，形成以互动驱动学习的教育新形态。最后，在数据安全治理方面，研究强调技术赋能必须以伦理与安全为前提，建立完善的数据保护、算法审查与责任追溯机制，确保教育智能化发展在法治与伦理框架内有序运行。总体来看，大语言模型不仅为高校安全教育提供了新的技术范式，更推动了教育理念的更新与教学生态的重构。

（二）研究展望

尽管本文从理论层面对大语言模型赋能高校安全教育进行了系统探讨，但仍存在进一步拓展的空间。未来研究可从以下几个方向深入：

1. 跨学科融合研究。应结合教育学、心理学、网络安全与人工智能伦理等多学科理论，构建综合性研究框架，为高校安全教育的智能化提供更加系统的理论支持。

2. 教育伦理与政策保障。需进一步完善 AI 参与教育伦理规范与监管政策，明确数据安全责任与算法透明标准，防止技术中心化倾向削弱教育的人文属性。

3. 教师能力建设。未来高校应重点加强教师 AI 素养培训，提升教师在智能教育环境中的引导力与判断力，形成人机协同、共育安全意识的教学格局。

参考文献

- [1] 曾建光, 尤澜涛, 严江南, 等. 思政创新与大语言模型“幻觉”——基于大语言模型中文评价平台的证据 [J]. 产业经济评论, 2025, (04): 180–200.
- [2] 卢晓涵, 安巧珍. 数智时代大学生法治素养培育的风险审视与引导策略 [J]. 学校党建与思想教育, 2025, (18): 70–72.
- [3] 李燕, 李玲. 数字技术赋能听障大学生心理健康教育的作用机理、现实困境与行动路径 [J]. 中国特殊教育, 2024, (11): 3–9.
- [4] 许立君, 杨丽, 黄子伟. 大语言模型与开源生态协同的人工智能课程创新探索与研究 [J]. 华东师范大学学报 (自然科学版), 2025, (05): 66–75.
- [5] 侯迪迪, 洪少东, 付玉杰, 等. 基于大语言模型链接的网络安全实体识别方法 [J]. 计算机应用, 1–12[2025–10–16].
- [6] 习近平谈治国理政 (第1卷) [M]. 北京: 外文出版社, 2018.
- [7] 李典, 李阳. 新时代大学生安全教育学与管理策略——评《大学生安全教育》[J]. 中国安全科学学报, 2025, 35(05): 264–265.
- [8] 倪皓. 法治视角下大学生法律意识培养创新研究——评《高校大学生安全教育和法律意识培养研究》[J]. 教育发展研究, 2024, 44(18): 85.
- [9] 周光玲, 黄义灵. 大语言模型赋能高校思政课教学探究 [J]. 学校党建与思想教育, 2025, (13): 70–73.
- [10] 陈启, 刘德喜, 张丽园, 等. 人工经验 + LLMs 智能: 基于支持策略规划的心理健康支持生成框架 [J]. 中文信息学报, 2025, 39(01): 153–166.
- [11] 张丽园, 刘德喜, 陈启, 等. 披露主题引导的在线心理健康支持回答生成 [J]. 小型微型计算机系统, 2025, 46(10): 2351–2363.
- [12] 杨莹. 大学生心理健康教育对安全行为的提升策略——评《安全行为心理学》[J]. 安全与环境学报, 2024, 24(09): 3704.
- [13] Shangase K K, Mokhethi K. Personal Listening Devices and Hearing Health: The Psychological and Social Factors Influencing Undergraduate Students’ Safe Listening Behaviors[J]. International Journal of Behavioral Medicine, 2025, (prepublish):1–11.
- [14] 李红霞, 韩明娟, 刘芳蕾. “三阶五段”教学模式的构建与实践——以国家级一流本科课程“大学生国家安全教育”为例 [J]. 中国大学教学, 2025, (09): 71–79.
- [15] 高远民, 王勇刚, 刘和剑, 等. 高校安全教育实验室建设与探索 [J]. 实验室研究与探索, 2025, 44(06): 239–244.
- [16] North C, Cosgriff M, Boyes M, et al. The work that the law does in education outside the classroom: part 1 – the law and student safety[J]. Journal of Adventure Education and Outdoor Learning, 2025, 25(3): 797–813.
- [17] 张树启. 移动互联网时代大学生网络安全教育的策略研究 [J]. 学校党建与思想教育, 2022, (24): 63–65.
- [18] 杨鉴伟. 人工智能赋能“大学生安全教育”课程教学思考——评《大学生安全教育理论与实践》[J]. 安全与环境学报, 2024, 24(12): 4928.
- [19] 杜蕾, 何雯. 大语言模型对高校大学生信息素养教育的影响与启示——以 ChatGPT 为例 [J]. 新世纪图书馆, 2024, (05): 64–72.
- [20] Garcia A M, Culbreth D, Foxx P S, et al. Keeping students safe: the experiences of educators implementing monitoring applications in K–12 settings[J]. Education and Information Technologies, 2025, 30(14):1–31.
- [21] 李峰, 郭嘉悦, 胡新雨, 等. 大语言模型辅助情境化命题模式探索——以创造性思维测评为例 [J]. 中国考试, 2025, (09): 76–86.
- [22] 雷浩, 杨春明. 大模型时代的生成式课程实施 [J]. 教育研究, 2025, 46(08): 93–105.
- [23] 卢淑怡, 褚乐阳, 王浙栋, 等. 大语言模型赋能的创意写作: 应用框架与案例实践 [J]. 现代教育技术, 2025, 35(08): 25–35.
- [24] 高承海, 党宝宝, 王冰洁, 等. 人工智能的语言优势和不足: 基于大语言模型与真实学生语文能力的比较 [J]. 心理学报, 2025, 57(06): 947–973.
- [25] 马方原, 于伟. 面向大语言模型学习环境的小学语文教学路径变革 [J]. 教育科学研究, 2024, (09):57–64.