Guidance: Using Artificial Intelligence During Research Activities

Table of Contents

Purpose

The purpose of this guidance is to provide Virginia Tech researchers with information about ethical and compliance dimensions to consider when using artificial intelligence (AI) in research activities.

Scope

This guidance applies to Virginia Tech principal investigators and researchers who are considering using artificial intelligence during research activities.

Definition

Artificial Intelligence (National Institute of Standards and Technology):

(1) A branch of computer science devoted to developing data processing systems that performs functions normally associated with human intelligence, such as reasoning, learning, and self-improvement.

(2) The capability of a device to perform functions that are normally associated with human intelligence such as reasoning, learning, and self-improvement.

Responsibilities

Principal Investigator: The PI is responsible for understanding the AI tools they use in their research as well as complying with all university policies and applicable state, federal, and international regulations, including those dealing with copyright and other intellectual property.

Virginia Tech Research Team Members: Research team members who generate, acquire, and work with research data are responsible for understanding the AI tools they use in their research as well as complying with all university policies and applicable state, federal, and international regulations, including those dealing with copyright and other intellectual property.

Virginia Tech IT Security Office: The Virginia Tech IT Security Office is tasked with staying abreast of advances, novel threats, and emerging new security-related tools related to AI and providing security training, security tools, consultation, and guidance to researchers and department IT personnel in the changing landscape.

University Departments: Departments are responsible for regularly analyzing risks related to their technology assets, including the integration of AI tools and threats to AI models, using the Virginia Tech IT Risk Assessment Process.

Scholarly Integrity and Research Compliance (SIRC)

> **Privacy and Research Data Protection Program:** PRDP is responsible for providing guidance to researchers for implementing the appropriate confidentiality, privacy, and security protections when using AI tools to collect and process research data.

> **Human Research Protection Program:** HRPP is responsible for supporting researchers who incorporate AI tools in their research with meeting their ethical and regulatory responsibilities to human research participants.

> **Research Integrity and Consultation Program:** RICP is responsible for providing research ethics consultation services to assist researchers with identifying, analyzing, and resolving complex questions that arise when incorporating AI tools in the conduct and dissemination of research.

Guidance

At Virginia Tech, we recognize the rapidly evolving landscape of AI tools and their potential to advance knowledge, research, and scholarly work. We support the responsible and ethical use of AI tools to ensure ethical research and innovation.

Researchers intending to employ AI in research activities need to do so in compliance with Virginia Tech policies, applicable state, federal, and international regulations.

Ethical and compliance dimensions of using AI in research include, but are not limited to the following.

1. Data Ownership

Researchers who use AI tools, including software and technologies owned by a third party, are responsible for understanding who owns and has rights to the data provided as input as well as the research data generated as output. Virginia Tech Policy 13015 states that research data are owned by Virginia Tech for all projects conducted under the auspices of the university or supported wholly or in part with university resources. Therefore, it is important to be aware of and understand the Terms of Service for AI tools to ensure that Virginia Tech retains ownership of research data.

2. Data Privacy and Protection

Researchers using AI tools, including software and technologies owned by a third party, are responsible for understanding how the information provided to or collected by these technologies is protected and who has access to the data. The Virginia Tech Risk Classification Standard classifies Virginia Tech data into three risk categories (low, medium, and high) and outlines minimum security standards for each level of data. Data classified as low risk are intended for public disclosure and/or data where the loss of confidentiality, integrity, or availability of the data would have no adverse impact on the university mission, safety, finances or reputation. **Therefore, only university data classified as low risk may be shared with or entered into a generative AI tool such as ChatGPT when there are no vendor agreements or contracts in place to protect ownership and privacy of the data.** Using third-party technology without a vendor agreement or contract in place requires review and approval via the Virginia Tech 'Low- Risk, Low-Cost' process ([Low-Risk, Low-Cost Software](#)). If non-public information (medium and high-risk data) is to be accessed or shared with third parties, they should be bound by contract to abide by Virginia Tech's information security policies. Examples of medium and high-risk data include, but are not limited to research data that are not intended for immediate public disclosure, information protected by FERPA, HIPAA, GDPR, Export Control, the Common Rule, data protected by contract, intellectual property, or other agreements.

It is also important to note that when working with external collaborators, additional terms and conditions might need to be included in data use agreements to ensure responsible and ethical use of AI tools by collaborating researchers and organizations.

Researchers with questions regarding how incorporating AI into a research project might affect privacy and protection of research data can contact the Privacy and Research Data Protection Program (prdp@vt.edu).

3. Protection of Human Subjects

Researchers who use AI in their work with human subjects should be aware of the potential risks and limitations, and should ensure that research participants are fully informed.

Biased data: Datasets that are generated using AI can be biased because the data and algorithms used to create them can be biased. This will likely result in a dataset that is not representative of the population of interest, which limits the generalizability of research results. This bias can also lead to invalid conclusions resulting in harm to historically marginalized and vulnerable populations by perpetuating negative stereotypes, discrimination, racism, classism, sexism, and other problematic assumptions.

Inaccurate data: Information generated from AI is only as accurate as its training data. Currently there are no standards for the veracity of information generated by AI and researchers must be cautious. Researchers should validate all AI generated-data and results using reliable sources.

Secondary use of existing data: Research using AI-generated data is considered secondary use of existing data. If a researcher elects to use existing data for research purposes, it is important to know and validate the source of the data. If the dataset is publicly available and does not require special permission to access, the researcher should ensure the data come from a reputable source. The researcher should not assume that the data can be used for research purposes or that consent was obtained to use the data for research.

Privacy and confidentiality for human subjects: Federal regulations for the protection of human subjects (the Common Rule) require adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data. Entering data from human subjects into a third-party AI tool can make the data available to the public and open source, thus failing to provide adequate provisions to protect the privacy of research participants. Providing de-identified data to third parties via AI tools can still pose privacy risks if the dataset contains enough variables that, when combined with other publicly available data or additional data sources, can be used to reidentify individuals. The Common Rule also requires that participants be fully informed about all of the risks associated with participation in a research study, including risks related to loss of privacy and confidentiality.

Research participants instill their trust in researchers and Virginia Tech when they provide us with data and information. Often the data are sensitive, which comes with the expectation that we will protect privacy and confidentiality. In order to benefit from the use

of AI, researchers must educate themselves, stay informed, and understand their responsibilities to research participants.

Researchers with questions about the use of AI in projects that involve human subjects, can contact irb@vt.edu.

4. Authorship, Plagiarism, and Reproducibility

Researchers should consider the following questions before deciding to use AI to support their research.

Can AI be listed as an author?

No. There is a consensus among journals and research communities that AI models "cannot meet the requirements for authorship as they cannot take responsibility for submitted work. As non-legal entities, they cannot assert the presence or absence of conflicts of interest nor manage copyright and license agreements" (Committee on Publication Ethics [COPE], Authorship and AI tools | COPE: Committee on Publication Ethics, 2023; Zielinski et al., 2023; Flanagin et al., 2023).

The concept of 'responsibility' is more than just ownership, it also includes accountability. Generative AI cannot be an author "because any attribution of authorship carries with it accountability for the work, and AI tools cannot take such responsibility" (Nature, 2023, p 612; Hosseini, Rasmussen & Resnik, 2023). Accountability is an essential element of authorship because it communicates liability and public responsibility for the work.

How should AI use be reported in my research?

Transparent and complete reporting of methods and materials used is crucial in promoting reproducibility and replicability of research. Therefore, researchers should clearly cite AI tools that were used to write the manuscript, produce images or graphical elements of the paper, or collect and analyze data. The citation should describe which AI tools were used as well as how those AI tools were used to support the research. Some AI technologies have publication policies to which researchers must adhere and provide stock language that can be used to cite their tools. For example, OpenAI suggests the following, provided it is accurate:

> The author generated this text in part with GPT-3, OpenAI's large-scale language-generation model. Upon generating draft language, the author reviewed, edited, and revised the language to their own liking and takes ultimate responsibility for the content of this publication (OpenAI Publication Policy, 2022)

Is the content generated by AI tools accurate?

Content generated from an AI tool can be inaccurate and biased. It is important to validate AI-generated content using other reliable resources. Researchers are responsible for ensuring that AI-generated outputs are appropriate and accurate. Given validity concerns about AI-generated information, researchers should also avoid relying solely on generative AI for decision-making purposes.

What if an AI tool provides inaccurate information?
AI tools have the potential to introduce plagiarized, falsified, and fabricated content, but as is indicated above, AI tools cannot be responsible or accountable. Authors who rely upon AI generated material without confirming the accuracy of the information will open themselves up to findings of academic and research misconduct, should fabrication, falsification, or plagiarism be contained within those AI materials. Accuracy and integrity in scientific work remains the researcher's responsibility for which they are accountable.

Researchers with questions about the use of AI and its role in authorship, plagiarism, and replicability can contact integrity@vt.edu.

Virginia Tech TLOS provides additional guidance on use of AI at Virginia Tech: Considering Generative AI and ChatGPT at Virginia Tech | TLOS | Virginia Tech (vt.edu)

Given the rapidly changing landscape of AI, we expect this guidance to require continuous updates. If you have any questions or feedback, please reach out to the Privacy and Research Data Protection Program (prdp@vt.edu).

References and Resources

ANSI INCITS 172-2002 (R2007) Information Technology—American National Standard Dictionary of Information Technology (ANSDIT) (Revision and Redesignation of ANSI X3.172-1996)

Arizona State University. *Guidelines for Use of Artificial Intelligence (AI) in Research.* Retrieved December 15, 2023, from Artificial Intelligence | Research Integrity and Assurance (asu.edu)

The Common Rule: Title 45, Part 46 of the Code of Federal Regulations "Protection of Human Subjects".

COPE: Committee on Publication Ethics. *Authorship and ai tools.* (2023, February 13). Retrieved December 15, 2023, from Authorship and AI tools | COPE: Committee on Publication Ethics

Flanagin A, Bibbins-Domingo K, Berkwits M, Christiansen SL. *Nonhuman "Authors" and Implications for the Integrity of Scientific Publication and Medical Knowledge.* JAMA. 2023;329(8):637–639. doi:10.1001/jama.2023.1344

Hosseini M, Rasmussen LM, Resnik DB. *Using AI to write scholarly publications. Accountability in Research.* 2023 Jan 25:1-9. doi: 10.1080/08989621.2023.2168535.

Nature (2023, January 24). *Tools such as ChatGPT threaten transparent science; here are our ground rules for their use.* Retrieved July 10, 2023, from https://www.nature.com/articles/d41586-023-00191-1

Northwestern. *Using AI Tools in Your Research.* Updated November 20, 2023. Retrieved December 15, 2023 from https://libguides.northwestern.edu/ai-tools-research

Office for Human Research Protections (OHRP) *Considerations for IRB Review of Research Involving Artificial Intelligence.* Approved July 21, 2022. Retrieved December 15, 2023 from https://www.hhs.gov/ohrp/sachrp-committee/recommendations/attachment-e-july-25-2022-letter/index.html

Open AI Publication Policy: Updated November 14, 2022. Retrieved November 15, 2023 from Sharing & publication policy (openai.com)

University of North Carolina at Chapel Hill. *Generative AI Usage Guidance. Research Community.* Retrieved December 15, 2023 from https://provost.unc.edu/generative-ai-usage-guidance-for-the-research-community/

University of Washington. *Guide to Artificial Intelligence (AI) in Health Sciences Research.* Updated December 20, 23. Retrieved December 21, 2023 from https://guides.lib.uw.edu/hsl/ai#s-lg-box-31157585

Virginia Tech Low-Risk, Low-Cost Technology Purchase Program FAQ: Low-Risk, Low-Cost Software Purchase Program

Virginia Tech Risk Classification Standard: Virginia-Tech-Risk-Classifications.pdf (vt.edu)

Virginia Tech Policy No. 13015 Ownership and Control of Research Data, Results, and Related Materials: VT Policy 13015

Virginia Tech comprehensive list of IT Policies: Policies & Standards | Division of Information Technology | Virginia Tech (vt.edu)

Virginia Tech TLOS Guidance for Generative AI: Considering Generative AI and ChatGPT at Virginia Tech | TLOS | Virginia Tech (vt.edu)

Zielinski, C., et al. (2023, May 31) Chatbots, ChatGPT, and scholarly manuscripts: WAME recommendations on Chatbots and generative artificial intelligence in relation to scholarly publications. Retrieved July 10, 2023, from Chatbots, Generative AI, and Scholarly Manuscripts || WAME

Dates Approved/Amended

Initial approval 12/21/2023

02/13/2024 Approved amendment adding information about Virginia Tech's Low-risk, Low-Cost Technology review program.