NCAE-C Student Code of Ethics and Professional Conduct

As a cybersecurity student, you are expected to uphold a code of ethics and professional behavior that promotes the highest standards of integrity, honesty, trustworthiness, and professionalism. This code serves as a guiding statement to support ethical decision-making and help maintain the trust and confidence of your clients, colleagues, employers, and the public. The following are the principles of the cybersecurity student code of ethics and professional behavior for students attending NCAE-C schools:

1. **Respect:** Treat others with respect and honesty, including awareness of potential bias, fairness concerns, and limitations in AI systems. Critically assess AI outputs and consider how training data, model design, or deployment context may impact individuals or communities. Act in a legal and moral fashion regarding others. Respect the laws, policies, and regulations that govern your profession or institution, and do not engage in any activities that could be considered illegal or unethical.
2. **Professionalism:** Conduct yourself both in person and online in a professional manner when dealing with clients, colleagues, and the public. Your actions should be based on sound judgment, integrity, and the highest levels of ethical conduct.
    - Do not delegate ethical decision-making or professional accountability to automated systems. Apply critical evaluation and human oversight to AI-assisted work.
    - Act with professionalism, integrity, and honesty in academic and professional settings, and use artificial intelligence and emerging technologies appropriately, ethically, and transparently.
3. **Confidentiality:** Maintain the privacy and confidentiality of information, especially concerning protected health information, personally identifiable information, or intellectual property entrusted to you. Do not input sensitive, protected, or proprietary data into AI systems without explicit authorization and a clear understanding of the system's data handling and security mechanisms.
4. **Accountability:** Take responsibility for your actions and be accountable for any mistakes or errors that you make. Learn from your mistakes and take steps to prevent them from happening again. You remain accountable for verifying the accuracy, legality, and ethical implications of AI-assisted outputs. Claims of automation or system error do not absolve personal responsibility.
5. **Collaboration:** Strive to collaborate both online and in person with other cyber professionals to make the cyber world safer for all.
6. **Attribution:** Give credit to others for their work. Only use work created by others and generative AI with proper attribution* and explicit permission from your college, university, or employer.*
7. **Continuous Learning:** Continue as a life-long learner to ensure competency in the field. Share your knowledge with others and promote best practices.
8. **Reporting:** Report any unethical behavior you observe in the course of your work to the appropriate authorities, including misuse of emerging technologies that compromise privacy, fairness, academic integrity, or public trust.
9. **Ethical Use of Emerging Technologies:** Use emerging technologies responsibly, transparently, and in alignment with ethical, legal, and professional standards. Conduct that is unethical without technology remains unethical regardless of how it is performed.
10. **Ethical AI Design & Deployment:** Be transparent about AI use, capabilities, and limitations. Apply explainable, human-overseen (human in the loop) models using only lawful, consented, and traceable data. Monitor and mitigate bias, model drift, and adversarial risks. Maintain appropriate audit records, enforce accountability, respect user autonomy, uphold Intellectual Property (IP) rights, minimize environmental impact, and conduct regular ethics reviews and training.

* Clearly attribute all sources, including AI-generated content, datasets, models, tools, and code, in accordance with institutional, legal, and professional standards. When permitted, disclose the use of generative AI and, when appropriate, identify the system used and the nature of its contribution.