3357:13-19-33 Confidential Data and Artificial Intelligence (AI) Policy

(A) This policy establishes general guidelines to protect North Central State College's confidential, sensitive, and proprietary information from being improperly shared with an artificial intelligence (AI) system without express authorization. It applies to all employees, contractors, and institutional partners conducting college business.

(B) Definitions

(1) Artificial Intelligence (AI) Tools: Software that performs tasks, data analysis, and decision-making using machine learning algorithms. Examples of standard AI tools: CoPilot, Gemini, ChatGPT, and Perplexity. Contact Information Technology (IT) if you have questions about the use of other tools.

(2) Prompt: In AI, a "prompt" is the input (a question, command, statement, or code) that a user provides to a language model to elicit a specific response, guiding the AI to generate relevant output.

(3) File upload: An AI tool or chatbot with file upload means it can generate output by reading the data and documents provided by users.

(4) Confidential Data: Any information protected by federal or state law, including student records, employee data, and proprietary college information.

(C) Permissible Uses of AI

(1) North Central State College recognizes that AI has multiple legitimate and accepted applications that can improve college operations, which include **but are not limited to** the following examples:

(a) AI tools may be used to improve administrative efficiency by aiding in scheduling, records management, communications, and workflow automation when appropriate oversight, accuracy checks, and data protections are maintained.

(b) AI tools may be used to expand or improve student access to services such as virtual assistants provided that their use is transparent and includes meaningful human oversight.

(c) AI tools maybe utilized to draft preliminary communications, summaries, or other content, provided that such statements are thoroughly reviewed for accuracy before any dissemination.

(d) AI tools may support data analysis, forecasting, and reporting provided that proper data governance practices were followed.

(e) AI tools may assist faculty in the educational process, including assisting with redesigning assignments, clarifying student instructions, generating test questions or study materials, and enhancing overall course quality. Such use must include transparency, accuracy checks, and appropriate academic oversight. Additionally, faculty must ensure no confidential information is shared with any AI program without express permission (see below).

(D) Responsible AI Use/Non-Permissible Use

(1) Employees must never input confidential, sensitive, or proprietary information into AI tools unless such input was approved by the college Institutional Review Board, See Policy 3357:13-12-10.

(2) AI tools are supplemental resources and should not replace human judgment or decision-making processes. Users must validate AI outputs before sharing, implementing, or acting on them. AI-generated content must be disclosed to stakeholders with appropriate disclaimers.

(3) Users are solely responsible for their use of the AI tool, and any actions or outputs generated do not reflect the beliefs, values, or official stance of the organization.

(E) Compliance with Laws and Regulations - All AI usage must comply with applicable laws and regulations, including FERPA, copyright, licensing, and other relevant state and federal laws.

(F) Training and Education – Employees will complete training provided by the College which will cover ethical use of AI, data security, and best practices for AI implementation upon being hired and annually thereafter.

(G) Consequences of Policy Violation - Violations of this policy may result in disciplinary action, loss of AI tool access privileges, or termination of employment, depending on the severity of the violation.

(H) Incident Response for AI Security Breaches - Any incidents related to AI tools, including unauthorized access, data leakage, or AI malfunctions, must be reported immediately to the IT department.

Effective: October 28, 2025
Next Review: October 1, 2030
Review Dates: 10/28/25