


Policy Name:	EMPLOYEE USE OF ARTIFICIAL INTELLIGENCE FOR WORKPLACE TASKS	
Approved By:	Board of Governors	
Approval Date:	October 25, 2024	
Next Scheduled Renewal Date:	September 2029	
Policy Holder:	VP, Corporate Services	
Operational Lead:	Director, IT Department and CIO	
Policy Number:	ADM-015	

EMPLOYEE USE OF ARTIFICIAL INTELLIGENCE FOR WORKPLACE TASKS POLICY

1.00 PURPOSE

- 1.1 The purpose of this policy is to provide direction for the Coast Mountain College (CMTN) community when using artificial intelligence (AI) for their administrative work. The use of AI for academic purposes will be covered in a separate policy.

2.00 DEFINITIONS

- 2.1 In this policy, these terms are defined as follows:
- a. **Artificial Intelligence (AI) Tool** – A type of artificial intelligence technology that can generate content at the request of a user, including audio, code, images, text, music, and video based on data on which it has been trained. The tool can be used for editing functions.
 - b. **CMTN College Community:** Employees, contractors, sub-contractors, volunteers, agents, and members of the Board of Governors of CMTN.

3.00 POLICY STATEMENT

- 3.1 CMTN recognizes the opportunities and potential that AI tools represent, including time-saving efficiencies in administration. CMTN also recognizes that AI is a tool to assist in performing tasks, not a replacement for human creativity and judgment.
- 3.2 CMTN encourages experimentation and use within the boundaries of ethical and responsible use. The guidelines in Sections 6.00, 7.00, and 8.00 provide direction for the College community on using AI responsibly for their administrative work. Using AI tools ethically and responsibly means being aware of, avoiding, and mitigating the risks.
- 3.3 Employees are also reminded of the requirements of [ADM-003, Freedom of Information and Protection of Privacy Policy](#), which also apply to the matters set out in this policy.

4.00 RESPONSIBLE USE

- 4.1 When using or deploying an AI project or activity, employees must ensure that it is done responsibly and in alignment with the following considerations¹:
- a. Fair – Ensure that content from these tools does not include or amplify biases and that it complies with human rights, accessibility, and procedural and substantive fairness obligations.
 - b. Accountable – Take responsibility for the content generated by these tools. This includes making sure it is factual, legal, ethical, and compliant with the terms of use.
 - c. Secure – Ensure that the infrastructure and tools are appropriate for the security classification of the information and that privacy and personal information are protected.
 - d. Transparent – Identify content that has been produced using generative AI; notify users that they are interacting with an AI tool; document decisions and provide explanations if tools are used to support decision-making.
 - e. Educated – Learn about the strengths, limitations and responsible use of the tools; learn how to create effective prompts and to identify potential weaknesses in the outputs.
 - f. Relevant – Ensure that the use of AI tools supports user and organizational needs and contributes to improved outcomes for all; identify appropriate tools for the task; be aware that AI tools are not the best choice in every situation.

5.00 DEPLOYMENT

- 5.1 When deploying an AI project or activity, the department involved must notify the IT Department in advance of its intended use, and the following additional checks and balances should be incorporated into the deployment workflow:
- a. Define a clear purpose for the use of the AI tool.
 - b. Ensure that
 - i. the data outputs of the use of the technology are accurate and reliable
 - ii. CMTN best practices are being followed in terms of privacy
 - iii. all CMTN policies are being followed, and where unsure, seek guidance.

6.00 PRIVACY

- 6.1 Do not upload or share confidential personal health or proprietary information with a public AI tool.
- 6.2 If the project requires the use of confidential health or proprietary information, a privacy impact and data security and risk assessment must be completed.
- 6.3 Never upload or share personal health information with an AI tool where the information is in the custody of a partner health care institute. Any use of this information must be within the control of their services and policies.

¹ Government of Canada's recommendations for the responsible use of AI.

7.00 PRIVACY BY DESIGN

7.1 In all areas of AI use, follow the seven privacy-by-design principles:

- a. Be proactive, not reactive — preventative, not remedial.
- b. Lead with privacy as the default setting.
- c. Embed privacy into design.
- d. Retain full functionality, including privacy and security.
- e. Ensure end-to-end security.
- f. Maintain visibility and transparency.
- g. Respect user privacy — keep systems user-centric.

7.2 Privacy needs to be at the core of digital operations, and everyone needs to work to protect it.

8.00 GUIDELINES FOR DEPLOYMENT OF AI TOOLS

8.1 Understand and measure the impact of AI.

- a. Complete a privacy impact assessment (PIA) prior to deploying the tool.
- b. Provide training so that users can understand the tool.

8.2 Be responsible for CMTN records and data.

- a. Do not enter personal or sensitive information into generative AI tools. This includes information about employees, contractors, job applicants, and other contacts.
- b. Use appropriate records management practices with generated data.

8.3 Be transparent about uses.

- a. Describe how the tool will be used and its benefits.
- b. Understand the secondary uses of data entered into the tool.

8.4 Critically engage with generated data.

- a. Be aware of bias and ethical challenges of generative AI.
- b. Fact-check any generated "evidence."

9.00 FOR ADVICE

9.1 For technical advice and recommendations, contact the IT Department, and for privacy concerns or guidance, contact the Privacy Officer.

10.00 RELATED POLICIES, PROCEDURES, AND SUPPORTING DOCUMENTS

10.1 [ADM-003, Freedom of Information and Protection of Privacy Policy](#)

11.00 HISTORY

Created/Revised/ Reviewed	Date	Author's Name and Role	Approved By
Created	Oct. 25, 2024	Tracy Boyde, Director of IT and CIO	Board of Governors