



DRAFT Security Standard for AI Usage

Parent Policy:	Use of Information Technology Resources		
Standard Sponsor:	College Information Officer		
Standard Contact:	Manager, IT Security		
Stakeholders:	Okanagan College Users		
Approved by:	College Information Officer		
Effective Date:	TBD		
Last reviewed:	TBD	Scheduled review date:	TBD

1. Background and Purpose

- 1.1 Generative Artificial Intelligence (AI) refers to a class of technologies capable of creating new content, such as text, images, audio, video, code, and simulations, based on the data on which they were trained. These tools present significant opportunities for innovation, operational efficiency, teaching enhancement, and enriched student and employee experiences across Okanagan College (OC).
- 1.2 Generative AI is not a replacement for human judgment, creativity, or professional expertise. Its use must align with OC values, policies, and commitments to privacy and security.
- 1.3 This Standard emphasizes the responsible use of AI technologies at Okanagan College, focusing on risk management and privacy protection. Principles and Use Guidelines can be found here: [BC Model Principles & Guidelines for the Use of AI](#).

2. Risks Associated with Generative AI Use

2.1 Risks Related to Data Storage

Most generative AI tools store, reuse, or train on user-provided input. This creates several risks:

- a) **Disclosure of confidential, personal, or sensitive information:** Anything you enter into an AI tool, including student data, HR information, internal documents, financial details, or system information, may become accessible to third parties.
- b) **Exposure of intellectual property or proprietary OC materials:** Internal documents, unpublished works, and protected materials must not be shared with external AI tools without approved safeguards.

- c) **Uncertain and unverifiable privacy protections:** Even when tools offer “do not train” options, these settings may not fully mitigate exposure risks.

2.2 Risks Related to AI-Generated Outputs

AI-generated content may:

- a) Present inaccurate, biased, fabricated, or misleading information (“hallucinations”).
- b) Reflect systemic or embedded biases present in the training data.
- c) Present material that may inadvertently duplicate or transform copyrighted or unlicensed works.
- d) Generate insecure or flawed technical outputs (e.g., code that weakens cybersecurity controls).
- e) Be overly convincing while still being incorrect..

3. Guidelines for Mitigating Risks

3.1 Understanding the Tools and Remain Current

Before using any generative AI tool:

- a) Review its Terms of Use, data retention practices, privacy policy, and security considerations.
- b) Understand the tool’s capabilities, limitations, and risks.
- c) Complete relevant training or review resources.
- d) Stay informed as generative AI continues to evolve.

3.2 Determining Appropriate and Responsible Use

While using any generative AI tool:

- a) Ensure AI use is appropriate to your role, responsibilities, and OC policies.
- b) No confidential, personal, private, student-related, proprietary, or business information may be entered into public AI tools unless approved through the appropriate OC security and privacy processes.
- c) For tools used in an official OC capacity, consult IT Services to determine whether a Privacy Impact Assessment (PIA), security review, or procurement assessment is required.
- d) Use AI in ways that support, not replace, human judgment, relationship-building, and professional accountability.

3.3 Being Accountable for Use of Results:

While reviewing outputs from the use of any generative AI tool:

- a) Verify the accuracy, completeness, and appropriateness of all AI-generated content.
- b) Ensure that any outputs from results align with OC values, policies, and legal obligations.
- c) Review and revise final communications, decisions, or instructional materials before sharing if necessary.
- d) Recognize situations where AI use may introduce bias or inequity.
- e) Cite and attribute sources where appropriate (see plagiarism considerations below).

4. Plagiarism and Attribution Considerations

- 4.1 When AI-generated content is used in administrative, instructional, or academic contexts, AI users should:

- a) Disclose the use of AI tools whenever the AI's output forms more than a minor part of the final work or influences the structure, ideas, analysis, or wording of the submission.
- b) Not present AI-generated text, images, or code as original human work unless permitted by policy or course guidelines.
- c) If the AI tool produces content that is clearly based on an identifiable external source, cite that source using the relevant disciplinary citation standards. If no specific source can be identified, state that the AI tool did not provide source information.
- d) Follow disciplinary citation standards for disclosing AI use. Best practice information can be found on the Okanagan College Library resources

5. Prohibited Uses

5.1 Generative AI must not be used for:

- a) Entering or processing personal information, student data, health information, or sensitive HR information in Public AI systems.
- b) Uploading or sharing internal OC documents without approval.
- c) Making decisions that affect students, employees, or the public without human oversight.
- d) Generating discriminatory, harmful, or biased content.
- e) Producing or distributing content that violates copyright or licensing agreements.
- f) Bypassing OC security, privacy, or technical controls.

5.2 Okanagan College will follow government guidance on prohibited or high-risk AI tools. Any tools banned or restricted by provincial or federal authorities are also considered prohibited at the College.

6. Guidelines for AI Users at Okanagan College

6.1 For Employees

- a) In learning environments, integrate AI tools in ways that support learning outcomes.
- b) Where AI tools are integrated into the learning environment, communicate expectations clearly to students around appropriate use of AI tools, including what may be considered a violation of the Academic Integrity Policy.
- c) Model responsible and ethical use of generative AI.
- d) Use AI only within the bounds of privacy, security, and College policies.
- e) Maintain responsibility for accuracy and appropriateness of outputs.

6.2 For Students

- a) Adhere to the use of generative AI where permitted in course outlines and in compliance with the Academic Integrity Policy.
- b) Use AI as a learning aid, not a substitute for learning.
- c) Disclose AI use when required.

7. Support for the Appropriate Use of AI Tools

7.1 IT Services will:

- a) Provide general support, education, and security guidance.
- b) Evaluate AI tools requiring enterprise-level adoption.
- c) Maintain ongoing monitoring of emerging risks and opportunities.

- d) Oversee updates to these Standards as appropriate.

8. Continuous Improvement

- 8.1 Given the pace and evolving nature of AI development, these Standards will be reviewed and updated regularly to reflect:
 - a) New regulatory frameworks
 - b) Emerging ethical considerations
 - c) Evolving cybersecurity standards
 - d) Advancements in AI capabilities
 - e) Feedback from faculty, staff, students, Indigenous partners, and equity groups
- 8.2 Okanagan College is committed to ensuring that the use of AI supports our mission, enhances learning and service, and respects the diverse communities we serve.

9. History / Revisions

Date	Action
------	--------

YYYY-MM-DD	New Standard Approved by : _____
------------	----------------------------------