

Policy Title: Artificial Intelligence Governance Policy		Policy Number: 149
Policy Category: Administrative		
Approval Date: May 1, 2026		Policy Owner: Corporate Services
Approved by: Chief Administrative Officer		File Reference: 0340-50

PREAMBLE

The Comox Valley Regional District (CVRD) recognizes that informed and responsible use of generative artificial intelligence (AI) applications can increase employee productivity and improve services. However, the use of AI also presents risks. Many of these risks arise from how generative AI applications function. Challenges include potential data errors, AI hallucinations (where AI generates responses with no basis in reality), lack of consistency in output, lack of transparency in how AI outputs are produced, the potential loss of empathy or individuality in communications, and ethical considerations such as bias, misinformation, and deepfakes. The use of generative AI applications also carries business and legal risk, including the potential for data privacy breaches, copyright violations, and issues related to the protection of confidential information.

Capitalizing on the capabilities and benefits of AI, while managing the risks, requires care on the part of all CVRD employees.

1. PURPOSE

- 1.1. The purpose of this policy is to guide employees on responsible, appropriate, and secure use of generative AI applications for CVRD business, and to provide protocols that maximize the benefits of using generative AI applications while managing potential risks and concerns.
- 1.2. This policy prohibits the use of AI for CVRD work activities, except as expressly permitted in this policy.

2. SCOPE

This policy applies to all CVRD employees' use of generative AI applications for any purpose related to their work for the CVRD, whether at CVRD offices or facilities, or from a remote work location.

The CVRD recognizes that there may be department specific generative AI needs and may make additional policies and procedures. Those additional policies and procedures are extensions of this policy and must be complied with, where applicable, unless an approved exception is granted.

3. DEFINITIONS

"AI" means Artificial Intelligence, the ability of digital systems to perform tasks typically associated with human intelligence, such as learning, reasoning, problem-solving, perception, and decision-making. This includes all forms of AI, including, but not limited to, machine learning and GenAI.

"AI Agent" means a dedicated AI tool designed to perform work on behalf of, or at the direction of a human, either interactively or autonomously.

"Approved AI" means platforms and technologies that have been approved for use by CVRD staff, or in public-facing applications, when used in compliance with this policy.

"GenAI" means Generative Artificial Intelligence, a subcategorization of AI that refers to the creation of new information (e.g., text, images, speech, or video) in response to a submitted prompt by learning from a large reference database of examples.

4. POLICY

4.1 Employees may only use approved AI platforms

Employees may only use the following generative AI applications for work-related purposes (collectively, "Authorized Generative AI Applications"):

- GovAI

Examples of prohibited platforms include, but are not limited to: ChatGPT, Gemini, Claude, Meta AI, and DeepSeek.

4.2 Training required before employee use of Authorized Generative AI Applications

Prior to using Authorized Generative AI Applications for any work-related purpose, employees must review and familiarize themselves with the Responsible Use of Generative Artificial Intelligence Guide attached to this Policy as Appendix A.

Employees are also encouraged to participate in continuing education or professional development programs related to generative AI as their manager considers appropriate.

4.3 All use of Authorized Generative AI Applications must comply with this policy

AI technology requires additional care to ensure privacy-sensitive, accountable, transparent and ethical application of the technology, such as the requirements laid out in this policy.

Examples of approved use include:

- Creating drafts of digital communications and reports before review and revision
- Reviewing and suggesting improvements to writing
- Providing ideas for avenues of research or thinking
- Summarizing documents or reports
- Interacting with an approved AI Agent

Examples of prohibited use include:

- Any use or procurement of AI platforms or technologies that are not Authorized Generative AI Applications
- Any use that results in unapproved disclosure of confidential information. Further information on confidential information is found in section 4.6.
- Any intentional use of sensitive personal information until reviewed by the Privacy Office. Further information on sensitive personal information can be found in section 4.7.
- Any use that results in AI responses being presented without CVRD employee review and personal accountability, except where authorized by the CVRD's Chief Administrative Officer (CAO)
- Any use that is in contravention of the CVRD Respect in the Workplace Policy and Staff and Volunteer Code of Conduct.

4.4 Employees are accountable for their use of Authorized Generative AI Applications

AI is a work aid and not a replacement for human judgment and expertise. Employees are solely responsible for their work product, including that generated or assisted by using AI tools.

GenAI has several shortcomings employees must be aware of when using it:

- GenAI is known to “hallucinate” and output content that appears legitimate but is completely fabricated (including references).
- GenAI tools are often trained on broad public documents, and as a result, responses can include inappropriate and implicit bias and dehumanizing tone.
- Reference materials for GenAI may not be current and may contain inaccurate information.

It is the sole responsibility of each Employee using AI tools to ensure that all content generated with the assistance of AI tools is accurate, reflects their professional judgement, appropriate communication style for the workplace, and aligns with CVRD corporate values, standards and policies.

4.5 Employees are responsible for transparent use of AI

As the use of AI evolves, it is important that its use is understood and shared across the organization to allow full benefits and to avoid unanticipated harms.

Employees are broadly encouraged to explore potential uses of Authorized Generative AI Applications in their existing work, within the parameters of this policy, and to share information about successful adoption with others across the organization.

4.6 Employees are responsible for ensuring no unauthorized disclosure of confidential information

Employees must ensure that AI outputs do not unintentionally include confidential information, and that any output containing confidential information is handled with the same care as the source material.

Confidential information includes any corporate information that an employee has not been authorized to disclose, and any personal information that is not business contact information. Some examples of confidential information include, but are not limited to, In-Camera or Closed Meeting materials and documents, legal opinions, corporate planning information, labour/employee relations information, third-party trade secrets and commercial information, and names, addresses or email addresses of employees or members of the public.

4.7 Use of Authorized Generative AI Applications with sensitive personal information requires additional review

The use of Authorized Generative AI Applications in conjunction with processes that routinely collect, use or disclose sensitive personal information requires review by the CVRD Privacy Office and, in many cases, will require the completion and approval of a separate Privacy Impact Assessment for that specific use.

The determination of sensitive personal information under the *Freedom of Information and Protection of Privacy Act* (FIPPA) is highly context sensitive. Examples include, but are not limited to, medical information, personal finances, sexual orientation, political beliefs, and other personal information that could present a higher risk of harm to individuals if improperly collected, used, or disclosed. More information on sensitive personal information can be found at the link below.

<https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/privacy-impact-assessments/guidance-on-disclosures-outside-of-canada#sensitive>

Please contact the CVRD Privacy Office if you have questions about sensitive personal information and before using Authorized Generative AI Applications for a process that routinely deals with Sensitive Personal Information. The Privacy Office can be reached at:

privacy@comoxvalleyrd.ca

4.8 Employees are responsible for records management of AI output

Like all CVRD records, the output of AI tools must only be stored in approved locations.

For general working (transitory) documents, this includes locations on the CVRD's network drives. Official records, such as records of decisions, must be stored in ELF or other approved CVRD systems (e.g., iCity, Vadim, LandUse, MARS, SharePoint etc.).

If transitory records are generated solely to support AI tools, such as transcripts used to support the creation of meeting minutes, summaries, or action items, these transitory records should be deleted as soon as the AI processing is complete to reduce overall storage costs and avoid over-retention of information.

Inputs and prompts into AI tools are considered transitory records and shall be retained no longer than 30 days.

4.9 New processes require privacy impact assessment

This policy authorizes the integration of Authorized Generative AI Applications into existing programs and procedures where no additional personal information is collected or disclosed, and where sensitive personal information is not involved, subject to the restrictions in this policy.

As required by FIPPA, any new initiative or substantive change to an existing initiative requires the completion and approval of a Privacy Impact Assessment.

If you are unsure whether your anticipated work may require a Privacy Impact Assessment, please contact the Privacy Office for more information at privacy@comoxvalleyrd.ca

4.10 Goods and services or solutions incorporating AI must not be purchased without approval

Contracted services that use AI, other than Authorized Generative AI Applications, may not be purchased by CVRD employees without prior approval of the Senior Manager of Information Systems and GIS.

Hardware or software solutions incorporating AI features may not be purchased by CVRD employees without the prior approval of the Senior Manager of Information Systems and GIS.

Employees anticipating procurement of goods and services or solutions incorporating AI are encouraged to contact the Information Systems and GIS Department well in advance of the planned procurement.

Where services or solutions contracted by the CVRD incorporate the use of AI without an opportunity for approval, for instance, a contractor adjusts how they perform a service to include AI without notice to the CVRD, this use must be curtailed, if possible, and reported to Senior Manager of Information Systems and GIS for review.

5. ROLES AND RESPONSIBILITIES

- a. The Chief Administrative Officer (CAO) is responsible for approving this policy and may amend or rescind at their sole discretion.
- b. The Senior Manager of Information Systems and GIS is responsible for reviewing and providing recommendations related to the use of AI at the CVRD, as defined in this policy. In this regard, the IT Steering Committee may be engaged for advice or recommendations for further AI use or implementation.
- c. All CVRD management staff are responsible for understanding their role and responsibilities under this policy and to communicate and enforce the consistent application of this policy within their areas of responsibility.

6. COMPLIANCE

6.1 Any breach of this policy will be investigated by Human Resources in collaboration with the Senior Manager of IT and the responsible manager and will be advanced in accordance with current collective agreements and/or corporate policy provisions, including the CVRD Progressive Discipline Policy.

REVISION HISTORY

Approval Date	Approved By	Description of Change

APPENDIX

Appendix A - Responsible Use of Generative Artificial Intelligence Guide

Appendix A

Responsible use of Generative Artificial Intelligence Guide

This guide has been developed based on available local government resources and in alignment with the [Government of Canada's Guide on the use of Generative AI](#) for Federal Institutions.

Purpose

The purpose of this guide is to provide CVRD employees with an understanding of key considerations in using GenAI tools to support their work. Employees are responsible for ensuring they adhere to all CVRD policies and applicable standards when performing all work-related activities.

As GenAI is a rapidly evolving field, these guidelines are interim and subject to revisions or replacement by future policies or standards as more knowledge about GenAI and its integration into the CVRD is obtained.

Prior to using any approved GenAI tool, staff are required to read and understand this guide. Staff are also encouraged to identify and explore additional learning and professional development opportunities associated with GenAI.

If you are unclear of your roles and responsibilities when using these tools, please contact your supervisor or manager to ensure you are compliant with all CVRD policies and procedures. As some services and processes may not be appropriate for use with GenAI tools, leadership may prescribe additional guidance and restrictions regarding how employees use GenAI to support their work.

Overview

GenAI is a type of artificial intelligence (AI) that can create realistic and diverse content, such as text, images, audio, or video. GenAI tools may change how people work, but they do not alter the value or impact of that work. When used thoughtfully, GenAI can improve productivity and creativity, help solve problems, and create new opportunities by supporting tasks and shifting effort toward higher-value and higher-priority activities.

While there are many opportunities associated with GenAI, it also poses ethical, privacy, social, legal, and security challenges and risks. It is therefore important to understand the principles, methods, and limitations of GenAI, as well as its potential. Staff must use these tools judiciously, upholding the integrity and values of the Comox Valley Regional District. Supported by the overarching policy,

this guideline addresses the responsible, appropriate, and secure use of GenAI powered tools for work purposes.

Common Challenges

- **Ethical:** It is important to consider the use of GenAI's impact on society, privacy, fairness, and other moral and ethical values.
- **Environmental:** Building, training, and using generative AI models requires the use of a significant amount of energy and water for cooling. For this reason, it is important to consider whether your use of AI is worth the environmental impact and to use generative AI tools as efficiently as possible.
- **Decision-making:** Using GenAI without adequate oversight, transparency and explainability causes errors, biases, and unfair outcomes. Note: GenAI must NOT be used to make any decisions, especially those decisions pertaining to services or funding.
- **Social:** Using GenAI to influence or replace human interactions, or to create/exacerbate social inequities. Generative AI tools can create realistic and convincing content that may be hard to distinguish from human-generated content. This poses a challenge for ensuring the authenticity, accuracy and accountability of the information shared and consumed online.

Common Risks

- **Privacy:** Using GenAI to collect, analyze, or share information about individuals or groups without proper consent, security, or accountability compromises privacy and data protection.
- **Legal:** Using GenAI in ways that are illegal or that pose challenges for legal responsibility, liability or enforcement presents the risk of violating or undermining existing laws, regulations, or rights.
- **Technology Security:** There is always a risk of data loss for any information input into or available to the GenAI and other technology tools.

Mitigating risks of using GenAI tools

Before using GenAI tools, CVRD employees must understand the benefits, risks, and how they can use generative AI tools to support their work responsibly.

Generative AI tools can generate inaccurate content, amplify biases, and violate intellectual property, privacy, and other laws. When CVRD employees use these tools, they must protect personal information and sensitive data.

To assist in mitigating risks associated with the use of these tools, it is recommended that employees restrict their use to activities where they can manage the risks effectively. To support staff in determining the level of risk, consider the following questions:

- Is there an existing process, procedure, or tool that I should be using instead of GenAI?
- Is the use of GenAI tools likely to increase productivity in a meaningful way?
- Is the use of GenAI tools for this purpose appropriate?
- Have I ensured that there will be human oversight over the GenAI output?
- Am I fully certain that no sensitive, confidential, or personal data is at risk of being compromised?
- How will I address the biases that may shape the generated content?
- Am I prepared to provide explanations for GenAI's use in my work?

Guiding Principles

1. Be accountable

Take responsibility for the content generated by GenAI tools. It is the responsibility of staff to verify and ensure the validity of outputs and that they are factual, legal, ethical, and compliant with CVRD policies and procedures. You can be open about the use of these tools in interactions with colleagues, service partners, and the public. This transparency builds trust and confidence in government use of data-enhanced technologies and encourages dialogue between technology users and those affected by it.

2. Foster equity and inclusiveness

Seek to understand how GenAI tools formulate responses and be mindful that GenAI responses have the potential for bias. GenAI tool results are based on patterns and relationships processed and synthesized from large datasets derived from existing human knowledge and AI generated information. These large data sets may contain errors, and are biased across race, sex, gender identity, disability, and many other factors.

3. Validity, trust and reliability

Staff must consult trustworthy sources to confirm that the facts and details in the AI generated content are accurate and trustworthy. Trustworthy sources include CVRD bylaws and policies, and provincial and federal legislation. Consult your supervisor or manager if you are unsure. Accurate and consistent information ensures the credibility of the CVRD.

4. Human-centric

CVRD staff are relied upon and trusted as stewards of public assets and property used to serve the residents of the Comox Valley. Human-centric AI focuses on ensuring systems and approaches align with human values, and experiences rather than treating efficiency as the main priority or objective. The use of GenAI tools must support the services provided by the CVRD to create strong, safe, and inclusive communities.

Sample Use Cases

GenAI can support the work of staff by creating original content such as text or images. GenAI tools have been trained on large volumes of data, including publicly available information from the Internet. Based on the training data, these models generate content that is statistically likely in response to a prompt (a set of instructions). Employees can improve the GenAI tool's response by refining prompts or asking the tool follow-up questions. Once a response is generated from the GenAI tool, staff must verify, fact-check, and research the output to ensure it aligns with the principles, best practices, and suggestions outlined in this guide.

Here are examples of ways staff can use GenAI to support their work responsibly:

1. Exploring and asking questions about new concepts
GenAI can provide summaries and explanations of various concepts, which staff can use as a starting place. Example: An engineering analyst hears about the value engineering method from a colleague. The staff member decides to use a GenAI tool. They describe to the tool: what they are doing to deliver a water services project, the challenges they are facing, and asks how value engineering could help. After some back-and-forth, the analyst identifies areas in which value engineering could assist and begins to explore other resources to advance its use.

2. Building structured information from informal summaries

With GenAI, you can describe a problem, situation, or task you've been faced with, and have it generate structured text, such as to-do lists, to help you organize your work.

Example: Throughout the day, an assistant receives several long and complex messages from their supervisor about various tasks that need attention. The assistant prefers structured to-do lists, so uses GenAI to generate a comprehensive to-do list based on the messages they received.

3. Feedback on written work

GenAI can be used to provide feedback on document drafts, enhancing clarity and coherence before they are reviewed by colleagues.

Example: A land use planner has drafted a presentation introducing the process for reviewing and updating an official community plan. For the audience, it will be the first time they've heard of this initiative. The planner provides the presentation to the GenAI tool and asks it to act as if it doesn't have any land use planning experience and to provide feedback based on what is and isn't clear. The planner uses the feedback as inspiration to make some wording changes for clarity.

Here are some examples of GenAI use that may be considered irresponsible or risky:

1. Over-reliance on AI for public communications

Using GenAI without adequate human oversight and review to draft communications can potentially cause harm to the public.

Example: During a severe weather event, a staff member hastily uses GenAI to create a communication updating the public on the status of the storm and available supports and services within the community. However, the lack of context-specific review results in unclear instructions to the public, causing confusion and risks to the safety of residents.

2. Inputting raw data into GenAI for analysis or summarization

It is unsafe to use GenAI to process data that contains sensitive or confidential information. GenAI tools cannot be relied on to generate output that does not contain traces of the sensitive data from the input.

Example: A staff member working on a housing study uses GenAI to summarize survey results for a staff report to the Board of Directors. In the output, the staff member fails to notice that the name of a precariously housed individual was inadvertently included, exposing personal details of a vulnerable individual.

Key contacts and feedback

Questions about GenAI tools or how to use them should be directed to the CVRD's Information Services and GIS Department at support@comoxvalleyrd.ca

Questions about access to information and protection of privacy should be directed to the CVRD's Privacy Office at privacy@comoxvalleyrd.ca

Have ideas for the next version of the Responsible Use of GenAI guide? Submit your feedback and ideas to support@comoxvalleyrd.ca