Use of Generative Artificial Intelligence (AI) Directive

1 SCOPE

1(1) Authority

This directive is issued under the authority of the Deputy Minister, Highways and Public Works, on April 30, 2026, in accordance with GAM 2.4: Information Governance.

1(2) Application

This directive applies to all government departments listed in General Administration Manual Policy 2.1.

1(3) Effective and review dates

(a) This directive takes effect on May 25, 2026.
(b) This directive will be reviewed annually. The next review is due on May 25, 2027.

1(4) Purpose

(a) This directive establishes the governmental requirements for the safe, responsible and ethical use of generative AI tools. It provides the foundation from which additional detailed policies, guidelines, standards and other tools may be developed.

(b) The purpose of this policy is to ensure that generative AI tools are used in accordance with the following principles:

- **Transparency:** We are transparent about our use of generative AI tools to promote accountability and maintain the public's trust.
- **Public benefit:** We leverage the use of generative AI tools in ways that improve efficiency and service delivery for the benefit of the public.
- **Responsibility and accountability:** We are responsible and accountable for all aspects of our use of generative AI tools.
- **Fairness:** We ensure that our use of generative AI tools does not amplify bias and reflects the Yukon's diverse population to ensure that no individuals or communities face discrimination or harm as a result of their use. We ensure its application promotes the values of equity and fairness.
- **Reliability:** We verify the accuracy of all AI outputs to ensure the information we use is reliable and trustworthy.

- **Safety and security:** We protect government information, including the personal information of Yukon citizens, and ensure that our use of generative AI tools is safe, secure and legal.

(c) This directive is to be read in conjunction with:

- Generative AI Guidance and Terms of Use for YG Employees (web resource)
- *Access to Information and Protection of Privacy Act* (ATIPPA)
- *Health Information Privacy and Management Act* (HIPMA)
- *Human Rights Act* (Yukon)
- Information Governance (GAM 2.4)
- Values and Ethics Code (GAM 3.63)

1(5) Definitions

(a) "Artificial intelligence (AI)": A branch of computer science that focuses on creating systems capable of performing tasks that would typically require human intelligence.

(b) "Confidential information": Government information obtained through employment and subject to ATIPPA and HIPMA. This includes, but is not limited to:

- personal information, including personal health information and personally identifying information;
- information subject to Cabinet confidence;
- information related to any known potential or ongoing legal action, even if not labelled confidential;
- proprietary information provided to the Yukon government in confidence by third parties; and
- anything that could impact intergovernmental relations or negotiations (including Traditional Knowledge or information that may be sacred, confidential or is otherwise owned by Yukon First Nations or transboundary Indigenous governments and groups).

(c) "Enterprise generative artificial intelligence (AI)": Generative AI tools that are customized to use an organization's data and integrated into the workplace.

(d) "Generative artificial intelligence (AI)": A subset of AI that produces content (e.g., text, images, video, audio, code) based on information or prompts submitted by the user.

(e) "Personal information": Has the same meaning as the *Access to Information and Protection of Privacy Act*.

(f) "Personal health information": Has the same meaning as the *Health Information Privacy and Management Act*.

(g) "Personally identifying information": Information that can be combined with other data to identify individuals or groups. The Yukon's small population and close-knit

communities mean that describing issues, characteristics or statistics alongside a community name or other details can risk identifying individuals or groups.

(h) "Record": Recorded information made or received by an organization during business and by reason of its activity, in digital or paper format.

2 ROLES AND RESPONSIBILITIES

2(1) Deputy heads will:

(a) Ensure employees read, understand and follow the requirements set out in this directive and adhere to all relevant legislation, guidelines and procedures related to the use of generative AI tools.

2(2) The Chief Information Officer, Highways and Public Works, will:

(a) Provide support services to departments, including:

- leadership on the implementation and evolution of this directive;
- interpretation of this directive's requirements;
- training, seminars, awareness and other forms of capacity building; and,
- guides and tools to support implementation.

(b) Support the Deputy Ministers' Review Committee in its leadership role by providing advice and briefing the committee (and other senior departmental decision makers, committees and council members) on issues, requirements, challenges, plans, progress and results related to this directive.

(c) Through the Office of the Chief Information Officer (OCIO), provide guidance by reviewing and approving select generative AI tools for enterprise use, at its discretion.

2(3) Departmental Information Technology (IT) representatives will:

(a) Review and approve select generative AI tools for departmental use, at their discretion and accounting for existing requirements, including Privacy Impact Assessments (PIAs) and Security Threat and Risk Assessments (STRAs).

(b) Recommend these tools to the OCIO **or** notify the OCIO of the use of these tools, in writing.

2(4) Program managers and supervisors will:

(a) Ensure employees are aware of the use of the generative AI directive, guidelines and related resources, including training.

3 REQUIREMENTS

3(1) Employees using generative AI tools for their work **may only use enterprise generative AI tools** that have been approved by the Office of the Chief Information Officer or

departmental IT representatives. A list of approved tools will be maintained on the "Generative AI Guidance and Terms of Use for YG Employees" SharePoint page.

(a) Confidential information may be entered into approved enterprise generative AI tools **only**.

3(2) Employees are responsible for verifying the accuracy, appropriateness and legality of any content generated by a generative AI tool, including the identification of bias.

3(3)(a) Generative AI outputs must be clearly cited when text is used verbatim, or near verbatim, or any imagery is used. For additional guidance regarding the use of AI-generated imagery, refer to ECO's **AI Image Guidelines**.

(b) Employees are required to appropriately manage and secure government records and information. Records created through the use of generative AI tools must be managed in accordance with the **Recordkeeping Guidelines for Generative AI**.

3(4) Employees must follow all relevant legislation, policies and guidelines when using generative AI. Employees should take available training to enhance their awareness and understanding.

(a) To ensure that the confidentiality of personal and personal health information is protected, employees must be familiar with and follow existing laws under the *Access to Information and Protection of Privacy Act* (ATIPPA) and the *Health Information Privacy and Management Act* (HIPMA).

(b) All standard policies and procedures respecting the implementation of new IT applications, software or systems continue to apply. This includes, but is not limited to, the requirements for completing a Privacy Impact Assessment (PIA) and Security Threat and Risk Assessment (STRA).

- Departments interested in integrating a new, unapproved generative AI tool into their business area can contact the Office of the Chief Information Officer for guidance on the steps that departments must take to assess its safety and security, including those listed above.
- Departments must not use unapproved tools until they have consulted with ICT, undertaken the required security assessments, and established the safety and security of the tool.

4 ENQUIRIES OR FEEDBACK

Questions or feedback on any aspect of this directive should be directed to the Chief Information Officer, Information and Communications Technology (ICT), Highways and Public Works.

REVISION HISTORY	Date	Notes
Version 1.0	May 7, 2026	Approved by Deputy Minister, Highways and Public Works