

Village Of Harrison Hot Springs Policy

POLICY NAME:	Generative AI and Information and Technology		
POLICY NUMBER:	1.44		
APPROVING AUTHORITY:	☒ Legislative (Council Approved)	☐ Administrative (CAO Approved)	
DATE ADOPTED:	July 13, 2026		
LAST AMENDED:			

PURPOSE

To establish guidelines for the secure and efficient use of generative artificial intelligence and technology resources within the Village of Harrison Hot Springs. This policy is intended to protect the integrity, confidentiality and availability of Village data while ensuring that any person accessing the network uses technology responsibly and in accordance with applicable laws and regulations.

DEFINITIONS

Authorized User means all employees, consultants, elected officials and any other person who uses municipal technology resources including hardware, software, networks and data systems

Copilot means the Generative AI service included with the Village's Microsoft licence agreement, the data from which is not used by Microsoft to train future Generative AI models

Device means an IT Resource used to connect to the Village Network, including but not limited to, desktop computers, laptops, tablets, cellphones or smartphones

Generative AI means software or services that use machine learning models to generate content based on user-supplied prompts, instructions or data

IT Resources means information and communication technologies including but not limited to information systems, Devices, software and networks owned or operated by the Village

Management means exempt employees of the Village who are excluded from the provisions of a collective bargaining agreement.

VPN means a secure, encrypted Virtual Private Network connection between an Authorized User's Device and the Village Network, allowing Authorized Users to access the network remotely

Village means the Village of Harrison Hot Springs

Village Network means all communications and connectivity infrastructure owned and managed by the Village, including but not limited to, wired and wireless networks, internet connections, local area networks, wide area networks, VPNs, servers, cloud services, and any other technology used to transmit, store or provide access to Village information

POLICY

1. Acceptable Use

- a. IT Resources are to be accessed primarily for official Village business purposes.
- b. Personal use of IT Resources should be limited, must not interfere with operations and must not violate any provincial or federal laws or regulations.
- c. Authorized Users must not:
 - i. Access, download or share inappropriate, illegal, discriminatory, explicit or offensive content;
 - ii. Use IT Resources for personal financial gain, political campaigning or any activity that may conflict with the user's official duties;
 - iii. Deliberately or carelessly propagate any virus or malware;
 - iv. Engage in unauthorized access or attempts to breach the Village Network; or
 - v. Install any unlicensed or unauthorized software.

2. Records Management

- a. Authorized Users must use their Village-assigned email and Village Network accounts when conducting Village business.
- b. Records produced using IT Resources belong to the Village and are subject to the *Freedom of Information and Protection of Privacy Act* [RSBC 1996] Chapter 165 as amended from time to time.
- c. Records produced using IT Resources must be retained on the Village Network and stored and disposed of in accordance with the Village's Records Management Bylaw No. 1030, 2013 as amended from time to time.
- d. Transitory records of temporary usefulness that are needed only to complete a routine action or prepare a subsequent record must be disposed of once no longer of value.
- e. Records produced using IT Resources must be stored on approved storage systems to ensure data security and reliability.
- f. Records produced using IT Resources must not be stored on personal devices, personal email accounts or unauthorized cloud storage services.
- g. Portable data storage devices, such as USB drives, should only be used if no suitable alternative exists and measures to encrypt or password protect the data should be taken.

3. Passwords/Authentication Credentials

- a. Authorized Users must be provided with unique and individually identifiable authentication credentials, such as a username and password, in order to access IT Resources and the Village Network.
- b. Authorized Users must not divulge, display, share or compromise their own or another Authorized User's authentication credentials except for the purpose of obtaining IT support from the Villages IT consultant or an otherwise authorized individual.
- c. Passwords must meet minimum complexity requirements and must be changed regularly.
- d. Two factor authentication will be required on an as-needed basis as determined by Management.

4. Data Security

- a. Sensitive and confidential data must be stored and transmitted securely.
- b. Access to sensitive and confidential data must be restricted to Authorized Users based on job roles, responsibilities and access requirements.
- c. Authorized User access and permissions will be regularly reviewed by Management.

5. Village Network Security

- a. The Village Network must be protected by firewalls, security measures, and intrusion detection and prevention systems to prevent unauthorized access.
- b. When accessing the Village Network remotely, all Authorized Users must only connect to the Village Network using a secure, authorized method such as VPN and two-factor authentication.

6. Device Security

- a. Any laptop or desktop computer connected to the Village Network will be protected by antivirus software and firewalls, as determined on a case-by-case basis by Management.
- b. Devices must be secured with passwords or biometric authentication before access to the Village Network may be granted.
- c. Authorized Users must not leave Devices unattended without taking appropriate security precautions when remotely logged into the Village Network, including locking the Device or disconnecting from the remote access when not in use.

- d. Where possible, Authorized Users accessing the Village Network remotely should connect to a secure, private or trusted internet network.
- e. Lost, stolen or compromised Devices must be reported to Management as soon as possible.

7. Generative AI

- a. Authorized Users may put confidential and personal information into Generative AI tools available to them as part of the Village's agreement with Microsoft and stored within the Village Network, such as Copilot.
- b. Authorized Users must not put any confidential information, including personal information, into publicly available Generative AI tools including but not limited to, ChatGPT or Google Gemini.
- c. Authorized Users who use Generative AI must review the outputs to ensure they are factually accurate, complete, compliant with intellectual property rights and use language that is inclusive, respectful and non-discriminatory.
- d. The use of Generative AI is intended to supplement and support employee productivity, not replace the employee decision making process. Authorized Users should not use Generative AI as a tool to obtain legal advice, make human resource decisions, complete procurement evaluations or make decisions affecting an individual directly.

8. Phishing or Suspicious Emails

- a. Authorized Users must exercise caution when accessing emails from unknown or unexpected sources.
- b. If an Authorized User receives an email that appears suspicious or may be a phishing attempt, they must:
 - i. Not click any links or open any attachments;
 - ii. Not provide any personal, financial or organizational information; and
 - iii. Delete the email.
- c. If an Authorized User clicks a link, opens an attachment or provides any personal, financial or organizational information and it is later determined to have been a suspicious email, the Authorized User must immediately report this to Management.

9. Monitoring, Incident Reporting and Investigations

- a. Use of IT Resources and the Village Network may be monitored, inspected or investigated by Management to ensure compliance with this policy or for any lawful Village business-related reason.

- b. While the Village respects the personal privacy of Authorized Users, it reserves the right to review the use of its IT Resources.
- c. Authorized Users should be aware that they have no right of ownership or expectation of privacy with respect to their use of IT Resources and use may be monitored to assist in protecting and maintaining the integrity and security of IT Resources.
- d. Authorized Users must immediately report any suspected or confirmed IT security incidents including but not limited to, data breaches, unauthorized access, malware attacks or inappropriate access, collections, use, disclosure or disposal of information to Management, who may investigate the matter at the discretion of the CAO or their designate.
- e. Authorized Users who fail to comply with this policy may be subject to:
 - i. Disciplinary action, including but not limited to dismissal or contract termination; or
 - ii. Suspension or revocation of access to IT Resources, the Village Network or Devices.

RECORD OF AMENDMENTS	
DATE AMENDED	SUMMARY OF AMENDMENTS