Town of Bon Accord
building for tomorrow

Policy 25-350

ACCEPTABLE USE AND INFORMATION SECURITY POLICY

SECTION: Administration / Council
DEPARTMENT: Administration
COUNCIL APPROVAL DATE: September 2, 2025
LAST REVIEWED BY COUNCIL: June 2, 2026

POLICY STATEMENT

The Town is dedicated to ensuring that Users have the necessary technology to maximize their efficiency and improve work processes. Employees are encouraged to utilize all internal computer-based technology (computer, email, internet, network systems) to the fullest to fulfill job requirements effectively.

PURPOSE

The purpose of this policy is to outline acceptable use for internet, email, devices, and passwords and ensure that Town IT resources are used appropriately at all times when conducting Town business. All Town information and correspondence, including email, transmitted/received is considered property of the Town and is to be managed accordingly for appropriate business-related matters.

SCOPE

This policy will govern the action of all Users in relation to any Town-owned or Personal Electronic Device while they are on the job or acting as a representative of the Town in any capacity, including the action of any volunteers and contractors while connected to a network owned/operated by the Town or while using any Town-owned equipment.

Users who are working remotely on Town devices must also ensure these practices are followed. Security of Town-owned Electronic Devices, equipment, and information will be governed by this policy in addition to the **Town Facilities Security Policy and Town-Issued Electronic Device Policy**.

Council approved September 2, 2025, Resolution 25-350
Council amended June 2, 2026, Resolution 26-123

DEFINITIONS

“Acceptable Business Use” means activities that directly or indirectly support Town business.

“AI” means artificial intelligence technology tools, including large language models (LLM), that enable computers to simulate human intelligence, allowing machines to learn, reason, solve problems, and make decisions.

“User" means any individual who is authorized to access Electronic Devices, including, but not limited to Town employees, Council members, volunteers, contractors, Bon Accord Public Library employees, Sturgeon County Fire Services employees, and those who have entered into facility rental contracts with the Town.

“Town-Issued Electronic Device” means a laptop, desktop, server, tablet, or smartphone that is Town-owned.

“Personal Electronic Device" means an Electronic Device that is not Town-owned.

RESPONSIBILITIES

Users utilizing the internet must conduct themselves in a professional manner at all times, especially while participating in collaborative activities, and must not disclose Town information or intellectual capital to unauthorized third parties.

Users are responsible for familiarizing themselves with procedures for downloading and protecting information in a secure manner, as well as for identifying and avoiding any online material deemed sensitive, private, or copyrighted.

I. ACCEPTABLE USE

1. Acceptable Internet Use

Designated Users may only use the internet to complete their job duties, under the purview of Town business objectives. Permissible, acceptable, and appropriate internet-related work activities include, but are not limited to:

a. Researching, accumulating, and disseminating any information related to the accomplishment of the user's assigned responsibilities, during working hours or overtime.

b. Collaborating and communicating with others according to the individual's assigned job duties and responsibilities.

c. Conducting professional development activities (e.g. news groups, chat sessions, discussion groups, posting to bulletin boards, web seminars, etc.) as they relate to meeting the user's job requirements.

2. Unacceptable Internet Use

Inappropriate and unacceptable internet use includes, but is not limited to:

a. Usage for illegal purposes, such as theft, fraud, slander, libel, defamation of character, harassment, stalking, identity theft, online gambling, spreading viruses, spamming, impersonation, intimidation, and plagiarism/copyright infringement.

b. Accessing, downloading, or printing any content that violates or conflicts with existing Town policies and/or engaging in any other activity which would in any way discredit, disrepute, or bring litigation upon the Town or harm its reputation.

c. Copying, destroying, or altering any data, documentation, or other information that belongs to the Town or any other business entity or individual without authorization.

d. Downloading unreasonably large files that may hinder network performance. All users shall use the internet in such a way that does not interfere with others' usage.

e. Engaging in personal online commercial activities, including offering services or products for sale or soliciting services or products from online providers.

f. Engaging in any activity that could compromise the security of Town host servers or computers.

g. Engaging in any fundraising activity, endorsing any products or services, or participating in any political activity, unless authorized to do so as part of completing one's assigned job duties and responsibilities.

h. Allowing unauthorized or third parties to access Town network(s) and/or resources.

i. Storing or downloading personal files or data on Town hard drives or network file servers.

j. Downloading video and/or sound files unless their use has been authorized for the purposes of conducting Town business.

k. Any online practices or procedures that would expose the network or resources to virus attacks, spyware, adware, malware, or hackers.

3. Personal Electronic Devices Use

a. Personal Electronic Devices may be used to access the following Town-owned resources for job related duties: email, calendars, and contacts.

b. Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing any Town resources, including email. (To jailbreak/root a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software.)

c. Only Town-Issued Electronic Devices (e.g.: laptops) may be used for remote login access to Town files.

d. Personal Electronic Devices may not be used to:

- **i.** Store or transmit proprietary information belonging to the Town or another company.
- **ii.** Infringe on individual privacy (e.g. record conversations or take photos).

e. See the Town's **Employment Policy** for details on the use of mobile devices and driving.

f. The abuse of personal internet use on Town-Issued Electronic Devices or Personal Electronic Devices during working hours will be subject to disciplinary action, up to and including termination of employment.

4. Artificial Intelligence (AI)

a. Employees may utilize AI for writing assistance to save time, including, but not limited to summarizing, rephrasing, creating ad copy, and letter writing.

b. Employees must use a Town-approved AI platform to ensure records and AI data flows can be replicated.

c. Employees are prohibited from inputting, uploading, or disclosing any of the following into AI tools:

   i. Personal Information;

   ii. Confidential or privileged information;

   iii. Non-public organizational information;

   iv. Information related to identifiable individuals, including residents, employees, contractors, elected officials or service providers; and

   v. Information subject to legal, contractual, or security restrictions.

d. Only an Employee with authorized access in accordance with the PIB may add the above information into the final document.

e. Employees are fully responsible for reviewing the entire contents of any information derived from AI tools for completion, accuracy, and bias.

f. The Town must inform individuals about the use of systems that use preset parameters where their personal information is processed. For example, the move-in script.

II. EMAILS

1. Email Usage

a. All Employees must use an approved method when accessing their email accounts. The list of approved methods are:

   i. Outlook Web Access

ii. Office 365 Login portal

iii. Outlook software installed on all Town-Issued or Personal Electronic Devices

b. Remote access to email is only authorized from locations within Canada. Locations outside the borders of Canada will be blocked. Use of a VPN or other method to bypass this filtering is not allowed.

c. Email cannot be used to send credit card numbers or other sensitive personal or financial information.

d. To help ensure compliance with Access to Information and Protection of Privacy legislation, all such related inquiries are to be forwarded to the Privacy Coordinator immediately.

e. An out of office message that includes an estimated return date (if possible) and details on contacting a secondary individual at the organization in case of an emergency, must be enabled for all planned absences.

f. The configuration of automatic forwarding rules to email addresses other than a Town email is strictly prohibited.

2. Phishing and Scams

Emails can host scams and malicious software. To avoid virus infection or data theft, Users should:

a. Avoid opening attachments or clicking on links when the content is not from a verified source.

b. Be suspicious of clickbait i.e.: offering prizes, too good to be true offers, etc.

c. Check email and names of people they receive a message from to ensure they are legitimate.

d. Look for inconsistencies, i.e.: grammar mistakes, capital letters, excessive number of exclamation marks, etc.

e. Forward suspicious emails **as an attachment** to the IT department with a brief explanation.

III. INFORMATION SECURITY

1. Data Transfer

Transferring data introduces security risks. Users must:

a. Avoid transferring sensitive data to other devices or accounts unless necessary.

b. Where possible, only share confidential data over the secure company drive.

c. Ensure recipients are authorized to receive the data being transferred, i.e.: double-checking email addresses before sending, etc.

d. Report scams, privacy breaches or hacking attempts as per the **Cyber Security Incident Response and Disaster Recovery Plan Policy**.

2. Additional Safeguards

To reduce the likelihood of a Cyber Security Incident, Users must:

a. Digitally lock all devices when leaving their desks e.g.: computers, tablets, smartphones, etc.

b. Ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area anytime they are expected to be gone for an extended period (e.g.: human resources papers are locked in a cabinet).

c. Ensure file cabinets containing restricted and/or sensitive information are kept closed and locked when not in use or when not attended, and associated keys are not left unattended.

d. Remove printouts containing restricted and/or sensitive information from the printer immediately.

e. Dispose of restricted and/or sensitive documents in the shredding bin.

f. Treat mass storage devices such as CD-ROM, DVD or USB drives as sensitive and secure them in a locked location.

g. Report stolen or damaged equipment as soon as possible to the Town Manager.

h. Change all account passwords at once when a device is stolen.

i. Report perceived threats or possible security weaknesses in Town systems.

j. Refrain from downloading suspicious, unauthorized, or illegal software on Town devices.

k. Avoid accessing suspicious websites.

IV. DEVICE SECURITY

1. Personal Electronic Devices

Users are expected to use their Personal Electronic Device(s) in an ethical manner at all times. Users who use Personal Electronic Devices for work must:

a. Report lost or stolen Personal Electronic Devices that contain ANY Town information (including email) to the Town Manager within 24 hours. Users are responsible for notifying their mobile carrier immediately upon loss of a device.

b. Not access Town information, including email, using a rooted (Android) or jailbroken (iOS) device. (To jailbreak/root a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software.)

c. Use the Town's secure WiFi connection while on site and use a secure WiFi or hardwired connection otherwise.

d. Personal Electronic Devices are not allowed to connect directly to any Town-Issued Electronic Devices. This includes, but is not limited to:

- **i.** Using a physical cable (USB, etc.) to connect to a Town-Issued Electronic Device to charge the Personal Electronic Device's battery.
- **ii.** Using software installed on a Town-Issued Electronic Device to perform a backup/sync (e.g.: iTunes).

e. Ensure the device locks itself with a password or PIN if it is idle for five minutes.

f. Inform the Town Manager as soon as possible if a User requires access to Town data outside of their designated parameters.

2. Filtering

The Town reserves the right to monitor and limit any internet activity occurring on its hardware, software, devices, equipment, and accounts. Specifically:

- **a.** The Town utilizes filtering to restrict access to websites deemed unsuitable for business use. Where the Town discovers activities that conflict with the law or this policy, internet usage records may be retrieved and used to document any wrongdoing.
- **b.** Individuals using Town hardware, software, equipment, devices and/or accounts to access the internet are subject to having online activities reviewed by IT personnel.
- **c.** Use of Town internet resources implies the user's consent to web monitoring for security purposes. All Users covered by this policy should bear in mind that internet sessions are likely not private.

3. Accessing & Monitoring Usage Records

The Town may access and monitor use of Town email and internet systems in the following ways:

- **a.** By monitoring email server performance and retained logs, backups and archives of emails sent and received through the Town server(s). Even when a User has deleted an email, the Town may still retain archived and/or backup copies of the email.
- **b.** By retaining logs, backups and archives of all internet access and network usage. These records may be audited, are subject to provincial, and/or federal laws and may be used as evidence. While individual usage is not routinely monitored, unusual or high-volume activities may warrant more detailed examination.
- **c.** By actively monitoring the traffic generated by devices owned by, or operating within networks owned by, the Town. Instances may include:
    - **i.** For the purposes of producing the email in response to a legal requirement or other lawful investigation.

ii. For the purpose of investigating whether there has been unacceptable use of email to abuse or harass other persons.

iii. For the purpose of investigating allegations of misconduct or to provide materials to external investigative authorities lawfully investigating possible criminal conduct.

4. Passwords

When creating passwords, Users should select passwords carefully and use common sense to avoid the risk of being easily hacked. Users must:

a. Choose passwords with at least eight (8) characters, including capital and lower-case letters, numbers and symbols, and avoid use of dates and other easily guessed verbiage i.e.: birthdays, pet names, iterations of the word “password”, etc. Choosing a passphrase is recommended. Please review the Government of Alberta Cybersecurity: Passphrases document for details on creating your passphrase.

b. Remember passwords rather than writing them down. If Users must write down or keep a record of passwords, they are obligated to keep the paper or digital document confidential and destroy it when it is no longer required.

c. Ensure passwords always remain secret. If a password must be disclosed to a trusted Town Employee or the Third-Party IT Support Provider, the User must reset the password and create a new password once the issue requiring the password has been resolved.

d. Change their password when prompted by the system.

e. Choose unique passwords for all Town accounts and may not use a password already in use for a personal account.

f. Not use the same password for different logins within the organization. Some resources can make use of the same user information (e.g.: Windows Login & Outlook), but if a new user needs to be created to access a certain resource, then a separate password must also be used.

g. Not reuse old passwords. When a password is changed it must be set to

something that was not used in the past. This will be enforced with software when possible.

h. Regularly change all passwords, with the frequency varying based on the sensitivity of the account in question (at least every 180 days). This will be enforced using software when possible.

i. Change a password immediately and notify IT if the security of a password is in doubt (e.g.: it appears that an unauthorized person has logged in to the account).

j. Change default passwords on the first login (e.g.: passwords created for new employees). This will be enforced using software when possible.

k. Not use password managers or other tools to help store and remember passwords without IT's permission.

5. Risks/Liabilities/Disclaimers

a. The Town reserves the right to disable access to an account and/or software without notification.

b. Users assume full liability for risks including, but not limited to, the partial or complete loss of Town-owned or personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the Device unusable.

REFERENCES:

Cyber Security Incident Response and Disaster Recovery Plan Policy

Employment Policy

Access to Information Act & Regulations

Protection of Privacy Act & Regulations

Government of Alberta Cybersecurity: Passphrases document

Town Facilities Security Policy

Town-Issued Electronic Device Policy

Council approved September 2, 2025, Resolution 25-350
Council amended June 2, 2026, Resolution 26-123