DISCOVER. GROW. BELONG.

Title: Internet Usage Policy	**Date Approved: January 9th, 2024**
Policy #: HR 02-2024	**Council Resolution #: 14-24**
Department: Human Resources	**Revision:**
Rescinds:	

Policy brief & purpose

Our employee internet usage policy outlines our guidelines for using our municipality's internet connections, network and equipment. We want to avoid inappropriate or illegal internet use that creates risks for our municipality's legality and reputation.

Preamble

This policy operates in addition to other policies, regulations and administrative directives for employees, as may be determined from time to time by council or the chief administrative officer.

Where any provision of this policy is inconsistent with a collective agreement or employment contract that applies to that employee, the provision of the collective agreement or employment contract applies.

Scope

This employee internet usage policy applies to all our employees, contractors, volunteers and partners who access our networks and computers.

Employee internet usage policy elements

What is appropriate employee internet usage?

Our employees are advised to only use our municipality's internet connections for the following reasons:

- To complete their job duties.
- To seek out information that they can use to improve their work.
- To access their social media accounts, while conforming to our social media policy.

We don't want to restrict our employees' access to websites of their choice, but we expect our employees to exercise good judgement and remain productive at work while using the internet.
Any use of our network and connection must follow our confidentiality and employee policies.

Carberry

DISCOVER. GROW. BELONG.

Employees should:

- Keep their passwords secret at all times.
- Log into their corporate accounts only from safe devices.
- Use strong passwords to log into work-related websites and services.

What is inappropriate employee internet usage?

Our employees must not use our network to:

- Download or upload obscene, offensive or illegal material.
- Send confidential information to unauthorized recipients.
- Invade another person's privacy and sensitive information.
- Download or upload movies, music and other copyrighted material and software.
- Visit potentially dangerous websites that can compromise the safety of our network and computers.
- Perform unauthorized or illegal actions, like hacking, fraud, buying/selling illegal goods and more.

We also advise our employees to be careful when downloading and opening/executing files and software. If they're unsure if a file is safe, they should ask their supervisor.

Our municipality may install anti-virus and disk encryption software on our municipal computers. Employees may not deactivate or configure settings and firewalls without CAO approval.

We won't assume any responsibility if employee devices are infected by malicious software, or if their personal data are compromised as a result of inappropriate employee use.

Municipal-issued equipment

We expect our employees to respect and protect our municipality's equipment. "Municipal equipment" in this computer usage policy for employees includes municipal-issued phones, laptops, tablets and any other electronic equipment, and belongs to our municipality.

We advise our employees to lock their devices in their desks when they're not using them. Our employees are responsible for their equipment whenever they take it out of their offices.

DISCOVER. GROW. BELONG.

Email

Our employees can use their municipal email accounts for both work-related and personal purposes as long as they don't violate this policy's rules. Employees shouldn't use their corporate email to:

- Register to illegal, unsafe, disreputable or suspect websites and services.
- Send obscene, offensive or discriminatory messages and content.
- Send unauthorized advertisements or solicitation emails.

Our municipality has the right to monitor corporate emails. We also have the right to monitor websites employees visit on our computers.

Disciplinary Action

Employees who don't conform to this employee internet usage policy will face disciplinary action. Serious violations will be cause for termination of employment, or legal action when appropriate. Examples of serious violations are:

- Using our internet connection to steal or engage in other illegal activities.
- Causing our computers to be infected by viruses, worms or other malicious software.
- Sending offensive or inappropriate emails to our customers, colleagues or partners.

Revisions

Council may, at its discretion and by resolution, amend this policy.

Adopted by Resolution of Council #14-24 at Carberry, Manitoba, this 9th day of January, 2024.