Mackenzie County

Title	Electronic Access and Acceptable Use Policy	Policy No:	ADM052

Legislation Reference	Municipal Government Act Sections 3 (a) (b) and 5 (b)

Purpose

A secure, sustainable and stable technological work environment requires information technology standards that are both enabling and responsible. The purpose of this policy is to identify access to technology for municipal purposes and to identify appropriate use of corporate technology.

Guidelines/Procedures:

This policy applies to all Employees and Elected Officials of Mackenzie County.

This policy pertains to various electronic devices provided by the Municipality for the purposes of conducting municipal business, which include, but are not limited to:

- Computers
- Laptops
- iPads and Other Tablet Devices
- iPhones, Smart Phones, and other cellular devices

Definitions:

"Electronic Devices" – includes, but is not limited to, computers, laptops, tablets, smart phones etc.

"Employee" – means all persons employed by Mackenzie County or an Elected Official elected to Mackenzie County Council.

"BYOD" – means Bring Your Own Device, in reference to personal devices used to connect to Mackenzie County communications services

"Municipality" – means Mackenzie County.

"IT Services" – Mackenzie County employees who are authorized to perform hardware and software maintenance on Mackenzie County computer systems.

1. Access to Communications

1.1 All electronic devices are Mackenzie County property. All applications and software purchased by the Municipality for use on electronic devices are considered Mackenzie County property. Upon termination of employment with Mackenzie County, all electronic devices and purchased software are to be returned to IT Services immediately, unless otherwise specified in this Policy.

1.2 The Municipality reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other County policies.

1.3 Employees should not assume electronic communications are completely private. Accordingly, if they have sensitive information to transmit, they should use other means.

2. Electronic Mail (Email)

2.1 Each authorized user must conduct himself or herself in a responsible and professional manner while using email.

2.2 Email messages, and any content or attachments contained in said email, which is marked as "confidential" must not be distributed or released unless you have the authority from the sender to do so.

2.3 County email is not to be used to forward spam, petitions, or pleas for help.

2.4 County email is not to be used to sign up sites or services for personal use. This includes but is not limited to: banking (including eTransfers), personal business or farm use, social media (ie: Facebook, Twitter, Linkedin, Pinterest, Instagram, etc), shopping (ie: Amazon, eBay, Costco, etc), streaming services (ie: Netflix, Spotify, Sirius XM, etc), or any other sites or services of personal interest. You must use your personal email to create logins for any sites that are not deemed necessary for County business.

2.5 County documents shall not be emailed to your personal email account unless approved by your supervisor.

2.6 Routine clean-up/archiving of emails is strongly encouraged to free up server space.

3. Lost, Damaged or Stolen

3.1 In the event that electronic equipment is lost, damaged, or stolen, IT Services must be contacted immediately.

4. Passwords

4.1 All user-level passwords shall be changed every 90 days, unless it meets the complexity requirements indicated below.

4.2 Passwords shall not be inserted into email messages or other forms of electronic communication (ie. chat, instant messaging).

4.3 If an account or password is suspected to have been compromised, report the incident to IT Services and change all passwords that may be affected.

4.4 Passwords must comply with the following complexity requirements:

a. Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
b. Be at least **ten** characters in length
c. Contain characters from **three** of the following **four** categories:
    i. English uppercase characters (A through Z)
    ii. English lowercase characters (a through z)
    iii. Base 10 digits (0 through 9)
    iv. Non-alphabetic characters (for example: !, $, #, %)

4.5 Passwords must be unique for each website and/or service; passwords must not be re-used.

4.6 A password app will be made available for staff and council members to keep track of passwords and for password collaboration in departments.

4.7 It is also strongly encouraged to set your electronic device to lock after 10 minutes of inactivity.

5. Personal Use

5.1 The electronic media and services provided by the Municipality are primarily for business use to assist employees and elected officials in the performance of their job duties. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-business purposes is understandable and all such use should be done in a manner that does not negatively affect the system's use for business purposes. Personal use of email must comply with section 2.4.

5.2 Personal use outside of a limited or occasional use should be with the expressed approval of an employee's supervisor. However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege. Email humor and jokes should be minimized to adequately comply with the provisions of the policy. Communications and information

research of a personal nature, not related to business activities, should be conducted outside normal working hours.

6. Portable Electronic Devices (tablets, phones, Laptops)

6.1 It is the responsibility of the user to ensure that municipal equipment remains in a good state of repair and that the following guidelines are followed:

- Usage of protective covers/cases. These will be provided to the user on initial distribution and should be used to prevent damage.
- The iPad and iPhone screens are made of glass and therefore are subject to cracking and breaking if misused. Never drop nor place heavy objects on top of the iPad or iPhone.
- Only use a soft cloth or approved laptop screen cleaning solution to clean the screen.
- Do not subject the iPad/iPhone to extreme heat or cold.
- Users may not photograph any other person, without that persons' consent.
- For security purposes, users must set a passcode on their assigned iPad/iPhone.

6.2 Some devices have cellular capability, however, users must access free wireless internet wherever possible to reduce the cost to the Municipality. A "data roaming block" will be placed on all iPads/iPhones which blocks data usage while a user is out of the country.

6.3 iPad users will be allowed a maximum data plan of $50 per month, any overages will be the responsibility of the Employee and deducted through the municipalities payroll system.

6.4 Designated personnel may be issued a cell phone or qualify to receive a monthly reimbursement for the purpose of conducting municipal business, see Schedule B attached. County Management shall be responsible for the authorizing and monitoring of Employee cell phone usage to ensure appropriate use and costs incurred are financially responsible.

6.5 The Municipality may approve the installation of various Apps in order for users to conduct municipal business. The cost of these approved applications may be submitted for reimbursement upon approval by their supervisor. (for example: Pages, Numbers, DocuMob, etc.)

6.6 Personal laptops, vendor laptops, and contractor devices or laptops not owned by the Municipality will not be allowed on Mackenzie County's network unless pre-approved by IT Services before each connection to the network.

6.7 Virtual Private Networking (VPN) access may be available to users that require network access outside the office.

6.8 When connected to the Municipality's network from inside/outside the office, it is the responsibility of the authorized user to adhere to this policy in its entirety and to ensure that family members, colleges, and general public do not gain access to the Municipality's network.

6.9 Mobile devices are kept on our persons, removed from company locations on a daily basis, and are in danger of being lost or stolen. Whenever sensitive business data is stored on the device, the mobile device must be password protected.

6.10 Never leave a portable electronic device in an unlocked vehicle, even if the vehicle is in your driveway or garage, and never leave it in plain sight. If you must leave your device in a vehicle, the best place is a locked trunk. If you don't have a trunk, cover it up and lock the doors.

7. Prohibited Communications

7.1 Electronic media cannot knowingly be used for transmitting, retrieving, or storing any communication that is:

- Discriminatory or harassing;
- Derogatory to any individual or group;
- Obscene, sexually explicit or pornographic;
- Defamatory or threatening;
- In contravention to a signed "confidentiality agreement";
- In violation of any license governing the use of software;
- Engaged in for any purpose that is illegal or contrary to Mackenzie County policy or business interests, or
- Used in such a way to damage the name or reputation of Mackenzie County, its employees, or elected officials.

8. Replacement

8.1 A replacement device shall be made available to the Employee in the event that the device becomes lost, damaged, or stolen.

8.2 In the event that the device is found to have been damaged as a result of neglect by the Employee, the Employee may be liable for the cost of replacement.

9. Security/Appropriate Use

9.1 Employees must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been

granted by County Management, employees are prohibited from engaging in, or attempting to engage in:

- Monitoring or intercepting the files or electronic communications of other employees or third parties;
- "Hacking" or obtaining access to systems or accounts they are not authorized to use;
- Using other people's log-ins or passwords; and
- Breaching, testing, or monitoring computer or network security measures.

9.2 No email or other electronic communications can be sent that attempts to hide the identity of the sender or represent the sender as someone else.

9.3 Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

9.4 Authorized users must respect the copyrights, software licensing rules, property rights, privacy rights and all federal, provincial and international laws.

9.5 All files and documents, whether in draft or final form, must be stored on the Municipality's network servers. Avoid storing files on the local drive of a computer system. If the user is working away from the office then files created or modified should be moved to the server as soon as possible. County servers are backed up nightly, allowing for recovery of data; whereas workstations/laptops are not backed up.

9.6 Personal files are not to be stored on the server. These can include, but are not limited to: personal photos or videos, music files, personal documents (such as your resume, or bank statements), or any other personal files not required for County business.

9.7 A Private folder is made available for each employee for storing work related private documents pertaining only to an individual employee. Examples may include your timesheets, time off requests, fuel sheets, or credit card reconciliation, etc. The private folder is not to be used for department related files or documents. If such documents need to be secured as private then a special area can be created by IT Services. For example, the Payroll department.

9.8 Municipal technology resources are to be used in a manner consistent with the Freedom of Information and Protection of Privacy Act and related County policies.

10. Softwareand Device/Cloud Storage

10.1 To prevent computer viruses from being transmitted through the County's system, unauthorized downloading of any unauthorized software is strictly prohibited.

10.2 Only software registered through or approved by IT Services may be downloaded. Employees should contact IT Services if they have any questions.

10.3 External storage devices shall not be used without consent by IT Services as they could contain viruses or malicious software. These include external hard drives, SD Cards, USB thumb drives, personal cameras, etc.

10.4 No personal network hardware should ever be connected to the County network, such as Wireless Access Point, Hotspot, router, switches, etc.

11. Technical Support

11.1 IT Services is authorized to:

- Determine the need for and permit an authorized user to access and use the internet and/or email through the Municipality's computer systems provided such access is restricted to municipal business purposes only;
- Arrange for training for authorized users;
- Assist in establishing rules, regulations, procedures and/or guidelines governing such access and use and the enforcement thereof;
- Deny, amend or revoke access by any authorized user and regarding any computer or group of computers in consultation with the Manager/Director or CAO;
- Make all users aware of the Electronic Access and Acceptable Use Policy.

11.2 IT Services shall satisfy that reasonable safeguards (hardware and/or software, encryption, passwords, etc.) are in place to adequately protect the Municipality's computers, computer systems, computer networks and all data and other information stored on or communicated through the computers, systems and networks from unauthorized access, theft, corruption, misdirection or any other reasonably foreseeable harm that may result from connection to the World Wide Web, the Internet or an external network.

12. Technology for Elected Officials

12.1 Elected Officials will receive and iPad with their assignment to municipal office.

- Computer or Laptop
- iPad

12.2 All technology equipment provided to an Elected Official must be returned or purchased at the end of their term of office or have the option to purchase their technology equipment at current fair market value. The decision to purchase equipment must be made as soon as practicable following a municipal election or upon resignation and prior to final payment being issued to the outgoing Elected Official.

12.3 Upon completion of a term in office all email data stored on Mackenzie County servers will be destroyed and the assigned iPad will be wiped unless it is purchased by the Elected Official.

12.4 Elected Officials have the option to purchase extended warranty for their iPad, at their expense.

12.5 Elected Officials are required to attend training sessions as necessary to become familiar with County technology equipment and acceptable use policies.

12.6 The minimum requirement for a BYOD device is the capability of:
a) Email access via connection to Microsoft Exchange
b) Form filling capability with PDF forms (for expenses)
c) Camera and audio for Zoom or other meetings (such as AUMA)
d) A modern browser for DocuShare access, etc.

13. Violations

13.1 It is a condition of using any of the Municipality's computers, computer systems or computer networks that any information created on, transferred to, transferred through, stored on or processed by any of the Municipality's computers, computer systems or computer networks is the property of the municipality and can be retrieved, examined, printed, copied, deleted, manipulated or otherwise dealt with by the Municipality without notice to anyone. The Municipality may, at its discretion, monitor, by a variety of means, the use being made of any of its computers, computer systems or networks to manage the systems, ensure their security and ensure compliance with this Policy.

13.2 The Municipality does not control material on the Internet and the Municipality is therefore unable to control the content of data or material that a user may discover or encounter through the use of the Internet. Authorized users are specifically prohibited from commencing, participating in or continuing any unacceptable use of any Municipal computer, computer system or computer network. Furthermore,

authorized users are responsible for ascertaining the accuracy or quality of information obtained through the Internet. Authorized users are encouraged to consider the source of any information they obtain and consider how valid that information may be prior to using or acting on it.

13.3 Any Employee who abuses the privilege of his/her access to electronic media and services in violation of this policy will be subject to corrective action, including possible termination of employment, legal action, and criminal liability.

14. Agreement

14.1 All Employees will be required to sign a copy of the "Electronic Access Use Agreement" (Schedule "A" attached) to acknowledge their understanding of the policy, its content and the consequence of uses that contravene this policy.

	Date	Resolution Number
Approved	07-May-13	13-05-328
Amended	11-Jun-14	14-06-409
Amended	7-Dec-21	21-12-821

Schedule “A”

Electronic Access Use Agreement

I certify that I have read, understand, and agree to the terms set forth in the Mackenzie County Electronic Access and Acceptable Use Policy in its entirety.

I further certify that I have received a copy of this Policy.

I acknowledge that the IT Administrator may remotely wipe my mobile device, if applicable, including all data (email, music, pictures, apps) if suspicious activity has occurred or the device has become compromised.

I acknowledge that using the Municipality’s systems is a privilege that may be revoked in the sole discretion of the Municipality for any reason, and that it automatically terminates when I leave the employment of the Municipality.

I hereby authorize the Municipality to deduct the amount in excess of the maximum data plan allowed, as stated in Section 6.3, through the Municipality’s payroll system.

Signature Date

Name (Please Print)

Schedule “B”

Persons Authorized to Receive Municipal Cell Phone or Monthly Reimbursement

1. The following personnel may be provided a municipal issued cell phone to conduct municipal business.

    - Chief Administrative Officer
    - Directors
    - Managers
    - Supervisors
    - Senior Utilities Officers
    - Lead Hands / Foreman
    - Fire Chiefs / Deputy Fire Chiefs

2. All other personnel requiring a municipal cell phone must obtain written authorization from their direct Supervisor and the Chief Administrative Officer.

3. Any Employee listed in Section 1 above may elect to use their personal cell phone and be given an appropriate monthly reimbursement as approved by the Chief Administrative Officer.

4. The following personnel may be provided a monthly reimbursement for utilizing their personal cell phones in order to conduct municipal business:

    - Fire Fighters $30.00
    - Equipment Operators $30.00
    - General Maintenance Laborers $30.00
    - Weed Inspectors $30.00
    - Seasonal Staff $30.00

5. All other personnel, not identified in Section 4 above, who are required to use their personal cell phone for municipal business must obtain written authorization from their direct Supervisor and the Chief Administrative Officer.

6. All Employees must complete the Employee Cell Phone Authorization Form (Schedule C attached) prior to receiving a municipal issued cell phone or monthly reimbursement.

7. Reimbursement for cell phones for Elected Officials is covered in the Honorariums and Related Expense Reimbursement for Councillor and Approved Committee Members Bylaw.

Schedule "C"

Employee Cell Phone Authorization Form

EMPLOYEE INFORMATION

Name: _____

Address: _____

Position/Title: _____

Department: _____

CELL PHONE OPTIONS

☐ **Option 1**

County Issued Cell Phone

Check all that apply:

- ☐ iPhone
- ☐ Smart Phone
- ☐ Mobile Phone
- ☐ Phone Case
- ☐ Car Charger
- ☐ Other _____

☐ **Option 2**

Personal Cell Phone

Please complete the following:

Cell Phone # _____

Monthly Reimbursement $_____

Employees must attach a copy of the first page of their personal bill as evidence of continued eligibility for cell phone allowance payments.

Signing authorizes the release of your number for internal use only.

APPROVAL

Employee Signature: _____

Date: _____

Supervisor Name: _____

Supervisor Signature: _____

Date Approved: _____

FOR OFFICE USE ONLY

County Issued Cell Phone Number _____

Financial Code/GL Account _____