ADMINISTRATIVE REPORT

Subject: Information Technology Resources Policy
Date: September 26, 2022
To: All Members of Council
From: Jeremy Hughes, IT Manager

FORTFRANCES
BOUNDLESS

ISSUE:

Amendments to the **Employment Standards Act, 2000** (**ESA**) require the Town of Fort Frances to implement a written policy with respect to the electronic monitoring of employees by October 11th, 2022.

ADMINISTRATIVE RECOMMENDATION:

THAT Council of the Town of Fort Frances agrees with the recommendation of Administration from **Item AR-22-0054** to implement the **Information Technology Resources Policy** as drafted.

STRATEGIC IMPACT:

- *Objective 19 - Improve information technology capacity*

OPTIONS & ALTERNATIVES:

1. Council authorizes the implementation of the **Information Technology Resources Policy** as drafted.
2. Council denies the authorization.
3. Council provides another direction.

HISTORY:

On April 11th, 2022, amendments to the **ESA** now require employers that employ 25 or more employees on January 1st of any year to have a written policy on the electronic monitoring of employees in place. In the first year of requirement, employers have until October 11th, 2022 to comply.

New Part XI.1 of the Act imposes requirements on employers to be transparent about whether they electronically monitor employees by:

1. Describing how and in what circumstances that monitoring occurs; and
2. Setting out the purposes for which the information obtained through the electronic monitoring may be used.

Two existing policies will be consolidated and replaced by the new **Information Technology Resources Policy** (3.20):

- **Internet / Email Acceptable Use Policy** (3.20)
- **Cell Phone Use Policy** (3.25)

ANALYSIS:

The existing **Internet / Email Acceptable Use Policy** (3.20) does not adequately address evolving requirements and privacy considerations that apply to Users accessing Information Technology Resources and Data.

The existing **Cell Phone Use Policy** (3.25) does not adequately address evolving requirements that apply to Mobile Devices deployed by the Town of Fort Frances to Users.

A new policy was drafted that considers these deficiencies and incorporates the new electronic monitoring requirements under the **ESA**.

This **ESA** does not establish a right for employees not to be electronically monitored by their employer and does not create any new privacy rights for employees. This policy does not change or restrict the ways in which electronic monitoring may take place.

The **Information Technology Resources Policy** will commence on a date no later than October 11th, 2022 and the Town of Fort Frances will provide the policy to all employees within 30 days of the policy's implementation.

CONSULTATION:

- Town of Fort Frances Senior Management
- Fort Frances Power Corporation Administration
- Fort Frances Power Corporation Board of Directors

SUPPORTING DOCUMENTS:

3.20 - Information Technology Resources Policy
3.20 - Internet Email Acceptable Use Policy
3.25 - Cell Phone Use Policy

FORTFRANCES
BOUNDLESS

INFORMATION TECHNOLOGY RESOURCES

HUMAN RESOURCES 3.20

POLICY

Created:	2022-09-19
Revised:	2022-09-22
Authorized:	Resolution X on YYYY-MM-DD
Superseded:	Resolution 150 on 2007-04
	Resolution 300 on 2009-10

1. PURPOSE

(1) This policy establishes controls governing the use of Data and IT Resources provided to Users from the Town by:

(a) Identifying the responsibilities of Users;

(b) Identifying prohibited User actions and ensuring the primary use of Data and IT Resources is for the Town's business activities;

(c) Protecting the confidentiality, integrity, and security of the Town's Data and IT Resources; and

(d) Informing Users about electronic monitoring.

2. APPLICATION

(1) This policy applies to all Users who:

(a) Create, distribute, access, or manage Data owned by the Town; and

(b) Access or manage IT Resources owned or operated by the Town, excluding:

(i) Members of the general public interacting with publicly accessible Town services.

3. PRIVACY

(1) The ***Employment Standards Act, 2000*** does not:

(a) Establish a right for employees not to be electronically monitored by their employer; or

(b) Create any new privacy rights for employees.

(2) IT Resources are Town property.

(3) IT Resources are provided to Users only so they can effectively conduct the responsibilities of their role with the Town.

(4) Users shall not expect privacy with respect to their use of IT Resources. Any use of IT Resources may be reviewed by the Town for the purposes outlined in Section 4.5 of this policy.

(5) Data stored on or created using IT Resources is Town property.

(6) The use of Credentials shall not create a reasonable expectation of privacy or confidentiality of Data.

(7) Access to Data may be granted to other Users through succession activities.

(8) Data is subject to relevant legislation and may be accessed by requests through ***The Municipal Freedom of Information and Protection of Privacy Act of Ontario***.

4. ELECTRONIC MONITORING

(1) The ***Employment Standards Act, 2000*** requires the Town to have a written policy on whether the Town electronically monitors employees, including:

(a) A description of how and in what circumstances the Town may electronically monitor employees; and

(b) The purposes for which information obtained through electronic monitoring may be used by the Town.

(2) The Town electronically monitors Users.

(3) Electronic monitoring Data may be captured using live telemetry and historical logs of:

(a) Software events, including but not limited to:

(i) Any event generated by any operating system or application installed on a Town device; and

(ii) Any event generated by any cloud application licensed or operated by the Town;

(Examples: launching Diamond from a Town workstation, making changes to an inventory record on CityWide from a personal smartphone, etc.)

(b) Network activity, including but not limited to:

(i) Attempts to access any Town network, device, or network location;

(ii) Information transmitted between any Town device and any network location (including the Internet); and

(iii) Information transmitted between any device connected to a Town network and any network location (including the Internet);

(Examples: signing into FMW from a Town workstation, uploading an EFT payment to a banking website from a Town workstation, watching YouTube from a personal smartphone connected to the Town's guest network, etc.)

(c) Communications, including but not limited to:

(i) Content and Metadata of emails and other messages sent or received by any Town device;

(ii) Metadata of emails and other messages sent or received by any device connected to a Town network;

(iii) Content and Metadata of emails and other messages sent or received by any cloud application licensed or operated by the Town; and

(iv) Content and Metadata of telephone calls sent, received, or forwarded by any Town telephone connected to a Town telephone system;

(v) Metadata of telephone calls sent, received, or forwarded by any Town Mobile Device;

(Examples: chatting through Teams from a Town workstation, sending email from a personal smartphone connected to the Town's guest network, receiving messages through When I Work, receiving voicemail from a desk phone at a Town workstation, timestamped logs of telephone numbers called from a Town smartphone, etc.)

(d) Physical movement, including but not limited to:

(i) GPS locations of Town vehicles and Town Mobile Devices; and

(ii) Attempts to access any secured Town facility or secured area in a Town facility;

(Examples: performing snow removal using a monitored Town vehicle, entering the Fire Hall outside of normal business hours, etc.)

(e) Video surveillance, including but not limited to:

(i) Images recorded by cameras at Town facilities; and

(ii) Images recorded by Town cameras in public spaces; and

(Examples: parking a vehicle at the Memorial Sports Centre, walking through the Rainy Lake Square, etc.)

(f) Use of input and output devices, including but not limited to:

(i) Cameras;

(ii) Scanners; and

(iii) Printers.

(Examples: accessing the Town's video surveillance infrastructure, scanning documents from a Town copier to a personal email, printing documents from a Town workstation, etc.)

(4) Electronic monitoring Data may be captured at any time.

(5) Electronic monitoring Data shall be used only for purposes that support the enforcement of this policy, including but not limited to:

(a) Protecting Data and IT Resources by investigating any security breaches, network anomalies, or violations of this policy as required;

(b) Preventing and responding to inappropriate or illegal activities;

(c) Administering Data and IT Resources, evaluating utilization, and planning for future use;

(d) Evaluating employee performance and supporting productive work environments; and

(e) Fulfilling freedom of information requests through ***The Municipal Freedom of Information and Protection of Privacy Act of Ontario***.

5. INCIDENT RESPONSE

(1) The IT Department shall always maintain unrestricted physical access to all physical IT Resources, excluding:

(a) Mobile Devices deployed to Users;

(b) Physical Credentials deployed to Users; and

(c) Physical IT Resources deployed within secured Water and Wastewater facilities.

(2) As necessitated by IT Department procedures, the Town may:

(a) Analyze electronic monitoring Data and share that Data with contracted third-party cybersecurity organizations;

(b) Limit any use of Data or IT Resources; or

(c) Recall, lock, or factory reset Mobile Devices at any time.

6. USER RESPONSIBILITIES

6.1. COMPLIANCE

(1) Users shall comply with all Town policies, procedures, and standards while using Data and IT Resources, including but not limited to:

(a) The ***Code of Conduct*** (By-Law No. 04/19);

(b) The ***Media Communication Policy*** (1.1);

(c) The ***Use of Corporate Resources in Election Periods Policy*** (1.17);

(d) The ***Employee Conduct Policy*** (3.7);

(e) The ***Social Media Conduct Policy*** (3.27);

(f) The ***Council / Staff Relations Policy*** (3.32);

(g) The ***Workplace Harassment Policy*** (5.34.1); and

(h) ***The Ontario Municipal Records Management System*** (By-Law No. 47-16).

(2) Users shall complete any security and compliance training prescribed by IT Department procedures.

(3) Users shall immediately report to the IT Department:

(a) Any inappropriate use of Data or IT Resources;

(b) Any lost, stolen, compromised, or damaged IT Resources; and

(c) Any loss, theft, or unauthorized disclosure of Data.

(4) Users shall comply with any investigation by the Town surrounding their use of Data or IT Resources.

(5) Users who violate this policy may be subject to appropriate actions, including but not limited to:

(a) Restriction, suspension, or revocation of access to Data or IT Resources;

(b) Disciplinary measures, up to and including termination of employment;

(c) Legal action, including damages, indemnification, or cost recovery; or

(d) Prosecution by local, provincial, or federal authorities.

6.2. LEGAL OBLIGATIONS

(1) Users shall comply with the laws and regulations of all applicable jurisdictions while using Data and IT Resources, including but not limited to:

(a) ***The Criminal Code of Canada***;

(b) ***The Copyright Act of Canada***; and

(c) ***The Municipal Freedom of Information and Protection of Privacy Act of Ontario***.

(2) Users shall adhere to all copyrights, patents, and licensing agreements for intellectual property licensed by the Town.

6.3. SECURING CREDENTIALS

(1) Users shall take every precaution reasonable to ensure their Credentials are always secure.

6.4. SECURING DATA

(1) Users shall utilize Data only for the purposes intended by the Town.

(2) Users shall take every precaution reasonable to ensure the Data they access is always secure.

(3) Users shall store and delete Data subject to the ***The Ontario Municipal Records Management System*** (By-Law No. 47-16).

6.5. SECURING DEVICES

(1) Users shall secure unattended devices in a manner that restricts access to them using only authorized Credentials.

(2) Upon the termination of their role with the Town, Users shall immediately return to the IT Department all physical IT Resources and physical Credentials issued to them by the Town.

6.6. SECURING MOBILE DEVICES

(1) Users may be assigned Mobile Devices to perform their role with the Town as determined by their supervisor in consultation with the IT Department.

(2) Users shall always maintain the enrollment of Mobile Devices in the Town's Mobile Device Management platform.

(3) Users shall always maintain the compliance of Mobile Devices with the configuration prescribed by the Town's Mobile Device management platform.

(4) Users shall take every reasonable precaution, with consideration given to their work environment and assigned tasks, to ensure Mobile Devices are always secure and protected from physical damage.

(5) Users may be invoiced by the Town for any Mobile Device costs the Town determines to be the result of personal use, including but not limited to:

(a) Enhanced device specifications;

(b) Usage overages; and

(c) Damage.

7. PROHIBITED ACTIONS

7.1. INAPPROPRIATE ACTIVITIES

(1) Users shall not use Data or IT Resources for purposes unrelated to the Town's business activities, including but not limited to:

(a) Commercial activities;

(b) Activities prohibited by Town policies or procedures; or

(c) Unauthorized charitable or not-for-profit activities.

(2) Users shall not use IT Resources for personal activities while on duty during working hours, including but not limited to:

(a) Activities that result in increased costs to the Town;

(b) Activities in locations that may disrupt the productivity of other Users;

(c) Social telephone calls or communications; or

(d) Playing games, watching videos, or browsing the Internet recreationally.

(3) Users shall not use personal email accounts to conduct the Town's business activities.

7.2. HARASSMENT

(1) Users shall not use Data or IT Resources to engage in harassment, including but not limited to:

(a) Cyberbullying;

(b) Fraudulent, abusive, malicious, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise inappropriate conduct; or

(c) Potentially offensive comments concerning religion, politics, or social policies.

7.3. DISRUPTION

(1) Users shall not circumvent or disclose any security measures implemented by the Town.

(2) Users shall not share or disclose any Credentials without authorization.

(3) Users shall not use Data or IT Resources for disruptive purposes, including but not limited to:

(a) Unauthorized access to IT Resources;

(b) Unauthorized impairment of IT Resources;

(c) Unauthorized deployment or removal of IT Resources; or

(d) Connecting unauthorized network or storage devices to IT Resources.

(4) Users shall not leave devices unattended in areas accessible by the public.

7.4. UNAUTHORIZED DATA USE

(1) Users shall not access nor attempt to access unauthorized Data, including but not limited to:

(a) Data not authorized for use by that User;

(b) Data protected under copyright law that is not licensed by the Town;

(c) Data that incurs usage fees that is not licensed by the Town; or

(d) Data that is obscene.

(2) Users shall not publish to any print or digital platform any unauthorized Data, including but not limited to:

(a) Images, video, or audio of individuals under the age of 18 without written consent of the parents or guardians of those individuals; or

(b) Images, video, or audio of individuals over the age of 18 without written consent of those individuals.

(3) Users shall not store Data on unauthorized devices.

(4) Users shall not attempt to nor successfully impair or exfiltrate Data.

(5) Users shall not destroy Data, except where authorized under the ***The Ontario Municipal Records Management System*** (By-Law No. 47-16).

7.5. USE OF MOBILE DEVICES

(1) Users shall not use Mobile Devices when it is unsafe to do so, including but not limited to:

(a) Non-firefighter Users operating vehicles;

(b) Firefighter Users operating vehicles while not responding to an emergency; or

(c) Connecting Mobile Devices to networks that are reasonably expected to be compromised.

(2) During offboarding procedures, Users shall not retain any telephone numbers of Mobile Devices assigned to them, excluding any telephone numbers released by Users to the Town during onboarding procedures.

8. DEFINITIONS

- **"Authorization"** means approval explicitly obtained from the IT Department, including but not limited to:
    - Configurations of permissions to IT Resources granted by the IT Department in consultation with a User's supervisor; and
    - Written requests for permissions from a User's supervisor to the IT Department.
- **"Credential"** means any method of authentication that grants access to otherwise restricted Data or IT Resources, including but not limited to:
    - Physical keys, proximity fobs, or hardware tokens;
    - Passcodes or personal identification numbers;
    - Combinations of usernames and passwords, or security questions and answers; and
    - Biometrics or gestures.
- **"Data"** means records stored on IT Resources, including but not limited to:
    - Documents;
    - Databases;
    - Media files;
    - Communications;
    - Metadata;
    - Location information; and
    - Activity logs.
- **"IT"** means Information Technology.
- **"IT Department"** means the IT Manager and any staff under the direction of the IT Manager.
- **"IT Resource"** means hardware, software, and networks, including but not limited to:

- Computing devices, such as servers, desktops, or Mobile Devices;
- Network devices, such as switches, access points, firewalls, printers, or scanners;
- Peripheral devices, such as mice, keyboards, docks, headsets, or cameras;
- Storage devices, such as hard drives, flash drives, tapes, disks, or optical media;
- Local services, such as applications, phone systems, network bandwidth, or storage; and
- Cloud services, such as Internet, email, collaboration tools, social media, or other digital assets.

- **"Metadata"** means Data that provides information about other Data, but not the content of that Data.
- **"Mobile Device"** means portable computing devices, including but not limited to:
  - Laptops;
  - Tablets; and
  - Smart Phones.
- **"Town"** means the Corporation of the Town of Fort Frances.
- **"User"** means individuals that access Data or IT Resources, including but not limited to:
  - Councillors;
  - Committee and board members;
  - Staff;
  - Volunteers; and
  - Contractors.

The Town of Fort Frances	**SECTION** HUMAN RESOURCES
INTERNET/EMAIL ACCEPTABLE USE **POLICY**	**NEW:** April 2007
Resolution No. 150 (Consent) 04/07	Supercedes Resolution No.
Policy Number 3.20	**PAGE 1 of 4**

I. POLICY SCOPE

This "Internet and Electronic Mail Use Policy" applies to all Town of Fort Frances (hereinafter "Town:) employees, guests and third-parties (hereinafter "Users") whose access to or use of Internet and email resources is provided by the Town of Fort Frances or available through equipment owned or leased by the Town of Fort Frances, whether or not that access is during normal working hours and whether such access is from the Town of Fort Frances's premises or elsewhere.

II. POLICY PURPOSE

This Policy is to establish guidelines and minimum requirements governing the acceptable use of the Town's Internet and electronic mail (Internet and email) resources.

By the Town establishing and maintaining compliance with this policy, the benefits of these communication tools can be realized while the risks and costs are mitigated. The objectives of this Policy are to ensure that:

- Use of the Town's email and Internet resources are related to, or for the benefit of the Town;
- Users understand that email messages and documents may be subject to the same laws, regulations, policies and other requirements as information communicated in other written forms and formats;
- Disruptions to the Town's activities from inappropriate use of the Town's email and Internet services are avoided; and
- Users are provided guidelines describing their personal responsibilities regarding confidentiality, privacy and acceptable use of the Town's Internet and email as defined by this Policy.

III. PRINCIPLES OF ACCEPTABLE USE

As with any resource provided by the Town, Internet and email resources should be dedicated to legitimate Town business activities and governed by rules of conduct similar to those applicable to the use of other information technology resources. The use of Internet and email resources imposes certain responsibilities and obligations on all Users and is subject to the Town's policies and procedures and all provincial and federal laws.

Acceptable use must be legal and ethical. Acceptable use demonstrates respect for intellectual property, ownership of information, network system security mechanisms, and individuals' rights to privacy and freedom from intimidation, harassment, and unwarranted annoyance. Furthermore, the nature of email raises expectations for a timely response — all Users are urged to read and respond to all email in a prompt and courteous manner.

All Internet and email use shall:

- Respect and uphold the law, including provincial and federal laws and regulations and the laws of other jurisdictions;
- Comply with the Town's stated policies, procedures and standards;
- Be courteous and follow accepted standards of etiquette;
- Protect others' privacy and confidentiality;
- Reflect responsible use of email and Internet resources and;
- Use information technology resources efficiently and productively.

IV. ACCEPTABLE AND UNACCEPTABLE ACTIVITIES

Acceptable Internet and email activities are those that conform to the purpose, goals, and mission of the Town and to each User's job duties and/or responsibilities. The following list, although not exhaustive, provides examples of *unacceptable* uses:

- Engaging in any illegal activity or using the Town's resources for any illegal purpose;
- Knowingly disseminating harassing, abusive, malicious, sexually explicit, threatening or illegal information, including jokes or cartoons;
- Using the Town's resources for purposes unrelated to the Town of Fort Frances's business activities, such as personal commercial use, advertisements, solicitations or promotions;
- Using the Town's resources to send messages expressing controversial, potentially offensive and/or defamatory comments of individuals, bodies corporate or groups including, but not limited to, religion, politics and social policies;
- Downloading or using the material, software or other intellectual property of others in violation of software licenses, copyright and trademark laws;
- Disclosing any passwords or security means and methods adopted by the Town;
- Allowing unauthorized persons to use the Town's computers or access the Town's network resources
- Attempting to circumvent any security measures put in place by the Town including attempting any unauthorized access to any data or information that is protected by passwords or other security measures
- Downloading or using any software not approved for use by the Town;
- Connecting any unauthorized equipment to the Town's network;

- Accessing any “chat” sessions including but not limited to MSN Messenger, ICQ, IM, etc.

Users may use the Town of Fort Frances’s Internet and email resources for incidental and occasional personal use, subject to the approval of the employee’s supervisor, provided that such use is reasonable in duration and is permitted, does not result in increased costs to the Town of Fort Frances and complies with this Policy, in particular Section V (Other Use).

Furthermore, Users must recognize that electronic correspondence is not inherently private, that messages could be misdirected and that the Town takes no responsibility resulting from the disclosure of private communications occurring over the Town of Fort Frances’s resources. Furthermore, the Town of Fort Frances retains the right to monitor any and all electronic communications and use of the Internet to ensure the integrity of the system and compliance with this Policy and to disclose when required or appropriate.

Furthermore, use of Internet and email resources may be subject to limitations as determined from time to time by the Town’s supervising authority. Users are advised to remove themselves from email and Internet lists not dealing with work-related topics.

V. OTHER USE

All use of the Town’s Internet and email resources for commercial purposes unrelated to the Town or for non-commercial, charitable or not-for-profit uses must first be approved in writing. Any such use must comply with this Policy.

VI. PRIVACY CONSIDERATIONS

Files in Users’ accounts and data on the network are regarded as personal: that is, the Town does not routinely monitor this information. However, the Town reserves the right to view or scan any file, email or software stored on the Town’s systems or transmitted over the Town’s networks and may do so periodically to verify that software and hardware are working correctly, to look for particular kinds of data or software (such as computer viruses or unauthorized software), or to audit the use of the Town ’s resources. Potential violations of this Policy that come to the Town’s attention during these and other activities may be acted upon.

Users must not send email messages containing unusually sensitive information over the Internet using any other method than the installed Lotus Notes email system. Furthermore, the Town of Fort Frances must be provided with a copy of all passwords and/or private keys needed to decrypt the communications and install software.

VII. SANCTIONS

Potential violations of this Policy may result in suspension of the User’s access to the Town’s Internet and email resources, followed by review of any costs and/or charges incurred by the Town.

Violations of this Policy may subject Users to the loss of Internet and email privileges and may result in disciplinary action, including termination.

Illegal acts involving the Town’s Internet and email resources may also subject violators to prosecution by local, provincial, and/or federal authorities. Suspected law violations may be referred to police agencies. The Town may seek legal action against any violators, including damages, indemnification and costs.

1. PURPOSE

The purpose of this policy is to offer guidance in the use and application of personal and Town of Fort Frances owned mobile phones.

2. AUTHORIZATION

The issuance of a Town of Fort Frances owned mobile phone must be approved by a Division Manager or the CAO. The use of a Town of Fort Frances owned mobile phone is considered a privilege and may be revoked.

Mobile phones will be assigned by need and not every employee will have a mobile phone assigned to them. Each case for a mobile phone will be reviewed individually and the business requirements, safety issues and appropriateness will all be taken into consideration when evaluating the need for a new phone.

Issuance of a mobile phone will be coordinated through the Manager of Information Technology when written (email acceptable) authorization has been provided.

3. USE

Business Use
Any mobile phone owned and issued by the Town of Fort Frances shall have as its primary function, business related uses.

Personal Use
This policy acknowledges that from time to time, a Town of Fort Frances issued mobile phone may be used for personal calls. As long as this use of the phone is incidental to its primary business use, personal calls are allowed.

If a situation occurs that warrants personal use of a Town of Fort Frances owned mobile phone beyond an incidental nature, the individual shall reimburse the Town, as appropriate.

Personal calls during designated work hours may not be taken at any time when it may disrupt the employee's assigned task / work and / or may compromise the safety of the employee, other employees, or the general public.

Typically, Town of Fort Frances phones may not be used for personal long distance or fee services. However, in an emergency situation, the expense for any such use shall be reimbursed to the Town as soon as possible. When practical, the employee must seek approval from their supervisor.

Meetings

Any individual using a Town of Fort Frances mobile phone shall use good judgment in how and where the phone is used. Phones taken into meetings shall be turned off or to vibrate. If a call is taken during a meeting, every effort should be made not to disrupt the meeting. Unless a call is specifically related to the topic of discussion, talking on the phone in a meeting is strongly discouraged.

Safety
Mobile phones may only be used when safe to do so and in accordance with any existing legislation regarding their use.

Use of Personal Owned Cell Phones
Employees not designated to carry a cell-phone for work purposes shall only use a personal cell phone contingent upon permission from his / her supervisor. This permission would be granted for special circumstances based upon personal need.

4. PHONE RECORDS

Every individual Town of Fort Frances owned mobile phone user is responsible for checking the accuracy of their bill before it is processed for payment. Discrepancies in billing data shall be resolved in a timely manner. If a Town of Fort Frances mobile phone is used for personal long distance or fee services, the Town of Fort Frances must be notified and the Town reimbursed.

In situations where cell phone usage exceeds the minutes provided by the cell phone plan a detailed call listing may be requested from the service provider. If it is determined that personal use has resulted a billing for additional minutes the user will be expected to reimburse the Town of Fort Frances for the additional costs. If it is determined that the additional minutes were for business use only then consideration should be given to changing to a plan with more minutes.

5. OTHER

The nature of the technology required to support the wireless mobile telephone is rapidly evolving. Phones may have additional features such as cameras, text messaging, Internet access, etc. The intent of this policy is to apply the principles enumerated herein to any such add – on or accessory feature.

6. CELL PHONE AND BLACKBERRY USE WHILE DRIVING

TOFF requires that all staff comply with applicable laws regarding mobile communications devices. Where operational needs require employees to be responsive to calls while in transit, employees shall pull over and stop the vehicle safely before placing, returning, or answering calls or messages. No attempt at talking, writing, texting, or other activities should be undertaken while in transit (either in personal or Corporation owned vehicles and equipment) that would distract the driver.

Legislation excludes Firefighters while performing their duties.