B.2.1

This document can be made available in other accessible formats as soon as practicable and upon request

STAFF REPORT: Finance & IT Services

REPORT TO:	**Committee of the Whole**
MEETING DATE:	**Monday, September 29, 2014**
REPORT NO.:	**FIT.14.49**
SUBJECT:	**Updated Information Technology Acceptable Use Policy**
PREPARED BY:	**Cathy Bailey, Manager of IT**

A. Recommendations

THAT Council receive Staff Report FIT.14.49 “Updated Information Technology Acceptable Use Policy”; and,

THAT Council approve the revised Information Technology (IT) Acceptable Use Policy as attached.

B. Background

In 2012, the current Information Technology Acceptable Use Policy, POL.COR.12.13, was approved by Council. This policy is to be reviewed every two years by the Senior Management Team. An updated version of the policy has been reviewed by the Information Technology (IT), Communications/Economic Development and Human Resources staff and then approved by the Senior Management Team.

The most significant changes to the policy are:

- An Introduction section has been added to provide general guidelines for staff.
- A section has been added to provide guidelines for exiting employees.
- Because social media forums are now taking on a bigger role, updates have been made that address staff use of these forms of communication while using Town computers.
- In an effort to reduce risk from virus infestations and loss of private data, wording has been added to prohibit the use of personal storage devices like USB keys, smart phones and music players on Town computers. Staff who can demonstrate a work requirement to use a USB key will be issued an encrypted key by IT. The purpose of this change is to ensure that technology is used in such a manner that private data entrusted to the Town is kept secure.
- Clearer wording has been added to make staff aware that sharing passwords is prohibited unless requested by IT or for IT approved group logins.
- Clearer wording has been added to make staff aware that performing Town work on a personal device is prohibited.

C. The Blue Mountains’ Strategic Plan

Strategic Goal 6 - Provide a strong, well-managed municipal government.

D. Environmental Impacts

N/A

E. Financial Impact

This is a risk management internal control to prevent potential financial loss.

F. In Consultation With

Tracey McKenna, Manager of Human Resources
Elizabeth Cornish, Communications and Economic Development Coordinator
Evan Davis, IT Technician

G. Attached

1. Information Technology Acceptable Use Policy

Respectfully submitted,

Cathy Bailey
Manager of Information Services

Ruth Prince
Acting Director Finance & IT Services

For more information, please contact:
Cathy Bailey
cbailey@thebluemountains.ca
519-599-3131 x. 257

TOWN OF THE BLUE MOUNTAINS

POLICY & PROCEDURES

Subject Title: Information Technology Acceptable Use Policy

Corporate Policy (Approved by Council)	X	Policy Ref. No.:	POL.COR.12.13
Administrative Policy (Approved by CAO)		By-law No.:	N/A
Department Policy: (Approved by Mgr.)		Name of Dept.:	Finance & IT Services
Date Approved: May 28, 2012		Staff Report:	FIT.12.17, FIT.14.49
Date Revised: September 29, 2014			

Policy Statement

This policy establishes guidelines for the use of the Town's corporate IT resources, including the acceptable use of Internet, E-mail, networks, computers, applications and mobile devices.

Purpose

The purpose of this policy is to:

- Ensure that technology is used in such a manner that the security of Town controlled data and equipment is maintained and respected.
- Ensure that technology is used in accordance with other existing Town policies.
- Emphasize the position of The Corporation of the Town of The Blue Mountains with regard to ethical conduct in the use of the Internet, E-mail and Social Media on corporately owned Internet connections, computers and mobile devices.

Application

This policy applies to all employees, volunteers and elected officials of The Corporation of the Town of The Blue Mountains, with respect to usage of the Internet, E-mail and Social Media on corporately owned computers and mobile devices such as, but not limited to, BlackBerrys, cell phones and Playbooks. It applies to Town IT equipment used both inside and outside of Town facilities, including at home and in any remote location.

Definitions

"CAO" means the Chief Administrative Officer of the Town or Designate.

"Department Head" means the Head of a specific Department, or CAO, who is responsible for a department budget for the Town.

"Designate" means the person(s) assigned the authority to act on behalf of the person charged with the principal authority to take the relevant action or decision.

"User" means employees, volunteers and elected officials.

"E-mail" includes all forms of electronic messaging, including the traditional Town E-mail system and social media forums like Twitter, YouTube, Instagram and Facebook.

"IT equipment" means all Information Technology which is corporately owned and on which users have access to the Internet, Intranet and E-mail. This includes, but is not limited to, desktop computers, laptop computers, as well as mobile devices such as BlackBerrys, cell phones, USB keys (jump drives) and tablets.

"IT Policy Form" refers to the IT Acceptable Use Policy Agreement Form (see Schedule A), which is used to track that a user has read and agrees to the terms in this Policy.

"MFIPAA" refers to the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56 (MFIPPA).

"Town" refers to the The Corporation of the Town of The Blue Mountains.

Procedures

Introduction

As an employee or an elected official of the Town of the Blue Mountains users are granted access to various technologies, tools, communications channels and databases in order to accomplish business objectives. User actions may affect the Town or the entities with which the Town does business. Users are expected to act in a manner that will promote the best interests of the Town.

Users must not use the Town's computer systems, Internet, E-mail or communications channels to:

a) Jeopardize confidential or personal information;
b) Embarrass or discredit the Town, our employees, officials or the persons with which we do business;
c) Violate legal or ethical standards;
d) Engage in activities while working that interfere with productivity;
e) Damage the Town's business relations or expose the Town to liability;
f) Act in an offensive, hostile, maliciously false, defamatory or unprofessional manner, or act on the Town's behalf without permission;
g) Share non-public information.

General Use and Ownership

1. The Town strives to protect the confidentiality of all network users, however, all information stored on the Town's systems is the property of the Town.

2. In the course of regularly scheduled activities, or specific investigation, the Town will have access to all information on any device belonging to the Town.

3. Personal information that is stored on any Town device will not be considered private.

4. Upon cessation of employment for any reason, any personal information stored on the Town's systems or devices may be forfeited and not returned to the user. The Town may, in its discretion, may make reasonable efforts to return any personal information stored on the Town's systems or devices, however, the Town reserves the right to charge a reasonable fee.

General Procedures

1. The use and disclosure of E-mail messages shall be covered under the provisions of MFIPPA.

2. E-mail messages shall be considered to be machine-readable records owned by the Town, for the purposes of MFIPPA, and as such will be considered electronic records.

3. The Town retains ownership in and shall have exclusive control over the reproduction of E-mail messages.

4. Messages that are transmitted to all users (Mail Users) or a large group of users must be urgent in nature and/or of general business interest to all users. Do not E-mail messages of a personal nature to large distribution lists.

5. Use of the network, E-mail, Internet or any IT device for any purpose related to a user's commercial business is not allowed.

6. Limited, occasional or incidental use of the network, E-mail, Internet or any IT device for any purposes other than for the business of the Town is acceptable, providing the privilege is not abused and that all other usage policies are adhered to.

7. Correspondence via Internet E-mail is NOT guaranteed to be private or confidential. Generally, information, which is sensitive or confidential in nature, should not be sent via Internet E-mail, unless the attached files are encrypted or password protected, since absolute privacy cannot be guaranteed.

8. Users are responsible for all electronic mail sent from their individual username and for all computer use while logged in under their username; all users should take appropriate precautions to ensure the passwords are changed regularly and not shared. Town IT Staff will set system policies that force passwords to be changed regularly. Sharing passwords is prohibited, unless using a group email account or when requested by IT staff.

9. Messages posted to Social Media web sites must conform to all Town standards, policies and regulations, including this policy.

10. Inappropriate uses of E-mail include:

    a) Messages that contain information which is, or may be, offensive or disruptive.

    b) Messages that contain information which is derogatory, defamatory or threatening in nature.

    c) Messages that contain information which is disseminated for a purpose which is illegal, or for a purpose which contravenes the Town's policies.

    d) Messages that reflect the personal opinions or biases of individual users or groups of users, and do not reflect official Town policies.

    e) Messages related to the operation of a user's personal business.

    f) Chain E-mail messages (chain letters).

11. The Town requires that users conduct themselves honestly and appropriately on the Internet, and respect the copyrights, software licensing rules, intellectual property rights, privacy and prerogatives of others, as in any other business dealing.

12. The Town reserves the right to blacklist or block any Internet site that it deems to be inappropriate or which may affect network performance.

13. In order to ensure security of Town resources, all non-Town owned devices (ie. computers, tablets, Blackberrys) that are to be connected to Town networks in Town facilities must be connected only to network jacks and wireless networks designated as public facilities.

14. Town staff using mobile computing devices such as notebook computers, tablets and Blackberrys must take every reasonable precaution for the security of these devices, including the use of strong passwords. In the event that a device is lost or stolen, Town IT Staff and the appropriate Department Head must be notified immediately.

15. Personal Devices:

    a) Connection of personal mobile storage devices like USB keys to your Town issued computer is prohibited. This includes personal USB keys, jump drives, smart phones and music players. Only encrypted USB keys issued by IT are permitted.
    b) Incidental to this, bringing files to work on USB keys from home computers is prohibited.
    c) Users may connect personal devices like smartphones and tablets to the Internet only via the network designated as public.
    d) Performing Town business on personal devices is prohibited.

16. Where practicable, files that contain information considered as private or confidential by MFIPPA must not be stored on mobile devices such as notebook computers, tablets, Blackberrys and USB keys or on third party off site servers. When private or confidential information must be stored on a mobile device or off site server, the device must be protected by the use of a password or encryption. In the event that a

device is stolen or lost and the device contains files considered private or confidential under MFIPPA, the appropriate Department Head must be notified.

17. Information considered as private or confidential by MFIPPA must not be posted to a Town web site or any other publicly accessible service, unless previously approved by IT staff and unless the data is protected by appropriate security.

18. The master copy of all corporate records and files must be located on Town servers and computers, not on third party off site servers, unless previously authorized by IT staff.

19. The following activities are prohibited at any time on IT equipment:

    a) Intentionally sending files or messages containing programs designed to disrupt other systems (commonly known as viruses);

    b) Accessing another computer system without authorization inside or outside of the Town's network (commonly known as hacking);

    c) Intentionally possessing, using, or transmitting unauthorized material, in violation of copyright restrictions;

    d) Installation of software in violation of software licensing and piracy restrictions;

    e) Creating, viewing, storing, printing or re-distributing unlawful or potentially offensive material or information, on any computer system accessed through the Town's network (this includes sexually explicit, obscene, or other potentially offensive material);

    f) Disclosing personal or confidential information to persons to whom it may not be disclosed under MFIPPA;

20. Any personal expenses incurred on an IT asset must be reimbursed to the Town by the user. This includes apps purchased or expenses incurred on a Blackberry or tablet computer.

21. The Human Resources Department is responsible to ensure that all users read and agree to the terms of this Policy before they are allowed to use any IT equipment. Completed IT Policy Forms (see Schedule A) for users are to be filed with Human Resources.

Exclusions

All of the following user groups are/will be covered under separate IT Acceptable Use policies:

1. The Blue Mountains Library staff
2. Public network users
3. Contractors, consultants and business partners engaging in IT business in Town facilities

References and Related Policies

POL.HS.10.12 Workplace Violence and Harassment Policy.

Consequences of Non-Compliance

All users should be aware that the Town's computer system creates records of every Internet site visited and every E-mail message sent.

If abuse of the Town's computer system is suspected, any Department Head or the CAO may request an audit of the suspected user's usage of the system. The Human Resources Manager and the CAO must approve this request in writing before IT staff performs an investigation under the direction of the CAO.

Details of the investigation, including any evidence, will be held in strict confidence and will only be shared on a limited need-to-know basis. If the investigation reveals that a compromise or breach of policy or legislation has occurred, it is the responsibility of the Department Head of the individual in question in consultation with Human Resources to determine if disciplinary action is required.

Failure to comply with this policy may result in disciplinary action up to and including termination of employment or cancellation of contract.

Review Cycle

This policy will be reviewed every two years by the Senior Management Team.

Schedule A
Information Technology Acceptable Use Policy Agreement Form

I/We have read and agree to follow and abide by the terms of The Corporation of the Town of The Blue Mountains IT Acceptable Use Policy

Name: ____

Date: ____

Signature: ____