Policy

POL.COR.12.13 - REVISED
Information Technology Acceptable Use Policy

Policy Type: Corporate Policy (Approved by Council)
Date Approved: June 20, 2022
Department: Finance and IT Services
Staff Report: FIT.12.17, FIT.14.47, FAF.17.154, FAF.18.80, FAF.20.19, FAF.22.103
By-Law No.: N/A

Policy Statement

This policy establishes procedures for the use of the Town of The Blue Mountains' (the "Town") IT Resources, including the acceptable use of Internet, Electronic Messaging, networks, computers, applications and mobile devices.

Purpose

Information Technology (IT) is an essential element in all Town operations. The objective of the Information Technology Acceptable Use Policy is to define the acceptable and appropriate level of business conduct required from the Users when using the IT Resources of the Town.

Application

This policy applies to all Users of The Corporation of the Town of The Blue Mountains' (the "Town") IT Resources operated by or on behalf of the Town. It applies to all information, in whatever form, related to the Town's activities, and to all IT Resources operated by the Town or on its behalf. It also applies to the User's use of the Internet, Electronic Messaging and other communication channels.

Definitions

"Attainable Housing Corporation" or "AHC" includes staff members and volunteers working for the Blue Mountains Attainable Housing Corporation, including the Attainable Housing Board members.

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

"CEO" means the Chief Executive Officer of the Library.

"Confidentiality" means ensuring that IT Resources are accessible only to those who are authorized to access.

"Contractor" means any third party vendor, Contractor or consultant who requires a system login to access Town IT Resources.

"Department Director" means the Director 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.

"Electronic Messaging" includes all forms of messaging, including the traditional Town e-mail system, instant messaging applications like Skype and social media forums like Twitter, YouTube, Instagram and Facebook.

"HR" means Human Resources.

"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.

"IT Resources" means all Information Technology, including the following:

- Information technology network, which includes its Local Area Network, Wide Area Network and all connected components, e.g., routers, switches, servers, hosts, storage devices, PCs, Mobile Devices (including cell phones and SmartPhones), tablets, and printers, etc.
- Operating System and software which includes all computer operating systems, systems software, applications software and any associated configuration parameters or files which affect the behaviour of these components.
- Cloud based systems and servers operated by the Town.
- Information hosted on the foregoing, including databases, files, email messages, text messages, Microsoft Teams Chat and Document Management System.
- IT Resources excludes equipment and software installed on the public network at the Library.

"Library Staff" includes staff members and volunteers working for the Blue Mountains Public Library, including the Library Board Members.

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

"Mobile Device" means any portable computing device installed with corporate standard software, supplied to a User by the Town for use in connection with the Town's business. Mobile Devices allow a User to connect from the office, home or while travelling. Mobile Devices include laptops, tablet PCs and SmartPhones.

“Portable Storage Device” or “PSD” is a removable electronic device that has only memory and can copy and store data. PSDs may include memory sticks and cards, USB flash drives, portable hard drives, CDs and DVDs.

“Town” refers to The Corporation of the Town of The Blue Mountains.

“User” means any person who interacts with the Town’s IT Resources and/or has access by any means to any IT Resources, including without limitation, employees and elected officials of the Town. It also applies to employees and volunteers of The Blue Mountains Public Library (the “Library”) and members of Boards and Committees who use the Town’s IT Resources.

Procedures

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. In addition, the size of personal storage on servers (I: drives) will be limited.
4. Upon cessation of employment for any reason, all personal information stored on the Town's systems or devices will be forfeited and NOT returned to the User. All devices and equipment must be returned.

Access Security

1. All Users will be provided with a personal User ID by IT staff. Users are responsible for all activities carried out with their personal User ID. Personal User ID passwords should never be shared with other Users unless asked by IT staff and only verbally. Users must not access IT Resources by using the personal User ID and password of any other User. The only exception to this is shared accounts used by groups of staff; these are not considered personal User ID’s.
2. Files kept on the local computer hard drive, computer desktop or mobile device are NOT backed up and cannot be restored if the device has a catastrophic failure. IT is not responsible for these files and may not be able to move them or restore them.
3. Users WILL NOT store files on their computer desktop. Putting temporary copies of working files on the desktop are acceptable, but master copies must be stored on a Town server. It is the User’s responsibility to ensure that data that is produced is on Town servers.
4. The following activities are prohibited at any time on IT Resources:
    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; and

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).

5. Personal Devices:

   a. Connection of personal mobile storage devices like USB keys to a Town issued computer is prohibited. This includes personal USB keys, external hard drives, jump drives, SmartPhones and music players. USB key use on a Town computer must be authorized by IT staff and will only be allowed after all other options are exhausted.

   b. Incidental to this, bringing files to work on USB keys or external hard drives from home computers is prohibited.

   c. Users may connect personal devices to the Internet only via the network designated as public.

   d. Performing Town business on personal devices is prohibited, with the exception of remote email services such as Outlook Web Access (OWA). While using OWA, Users must not save email messages, file attachments or documents onto their personal device.

6. Multi-Factor Authentication (MFA)

   a. All User accounts will be required to have MFA enabled for access to the Town Virtual Private Network (VPN) and email when not connected to the Town network at a Town Facility.

   b. Missing MFA Tokens must be reported to IT as soon as the device is noticed to be missing.

Information Confidentiality

1. Users must delete all Town data from their Portable Storage Devices as well as Mobile Devices, unless approved by IT, before discarding or handing the device over to any person or entity.

2. Users must exercise due diligence, as would apply in case of the Town's IT Resources, while dealing with the IT Resources of business partners, vendors, service providers, etc. with whom the Town has contractual relationships.

Internet and Electronic Messaging Use

Use of the Town's Internet and Electronic Messaging is intended primarily for Town business purposes. Personal use is permitted where such use does not affect the User's work performance, is not detrimental to the Town in any way, not in breach of any term or condition of the employment and does not place the User or the Town in breach of statutory or other legal obligations.

1. Users shall not use their Town email address for online services that are not Town business. For example, do not use a Town email address for shopping websites or social media services like Facebook or LinkedIn, unless they are authorized as Town business.
2. Users are accountable for their actions on the Internet and Electronic Messaging systems.
3. Users must use Internet and Electronic Messaging in a professional manner and in compliance with the legal, moral and regulatory codes of the country of use.
4. Users must not use Town Internet or Electronic Messaging to gamble, make personal gains or conduct a User's commercial business.
5. Users must not make official commitments through the Town Internet or Electronic Messaging on behalf of the Town unless authorized to do so.
6. Users must not download copyrighted material such as music files, video files or other large files unless they are specifically related to their job and are authorized to do so.
7. Users must use appropriate business language when sending Electronic Messages to colleagues or external parties. They must not use disrespectful, harassing, insulting or threatening language when communicating with colleagues or external parties.
8. Users must always use Town email addresses for Town communication. Users must not use any personal email addresses to send Town business related communications.
9. Users must not post, download or upload on the Internet or forward Electronic Messages containing inappropriate material.
10. Users must take extra care while accessing/opening Electronic Messages or attachments from unknown senders on either Town email or personal email accounts. Users must not follow the link(s) on spam messages.
11. Users must not use the IT Resources to send unsolicited messages (spam) to any internal or external address.
12. Users must not use the IT Resources, Electronic Messaging or other communication channels to:
    a. embarrass or discredit the Town, its employees, officials or the persons with which the Town does business;
    b. violate legal or ethical standards;
    c. engage in activities during work that interfere with productivity;
    d. damage the Town's business relations or expose the Town to liability;

e. act in an offensive, hostile, malicious, false, defamatory or unprofessional manner; or

f. act on the Town's behalf without permission.

13. 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 email messages of a personal nature to large distribution lists. This includes doing a Reply All to large numbers of recipients. Use blind copy (BCC) as much as possible when emailing to large numbers of Users.

14. Correspondence via Electronic Messaging is NOT guaranteed to be private or confidential. Generally, information, which is sensitive or confidential in nature, should not be sent via Electronic Messaging, unless the attached files are encrypted or password protected, since absolute privacy cannot be guaranteed. IT staff will have incidental access to messages sent and received while solving message delivery issues or during an authorized investigation.

15. Users are responsible for all Electronic Messaging 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.

16. Messages posted to Social Media websites on Town devices must conform to all Town standards, policies and regulations, including this policy and POL.COR.18.10, Social Media Policy.

17. Inappropriate uses of Electronic Messaging 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 messages (chain letters).

18. 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.

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

20. Users must not use publicly accessible file sharing services such as Google Docs or DropBox to send Town files to Internet Users. Only use IT approved services to share files.

Use of IT Resources

Users are provided access to IT Resources components based on their job role. Users must:

1. Connect/deploy only Town provided/approved IT Resource components (software or hardware) to the Town's network. Personal devices must only be connected to the Public network.
2. Exercise due care and diligence to safeguard IT Resources such as Town PCs, laptops and Mobile Devices from loss, theft, damage and unauthorized access; for example, SmartPhones must remain in a protective case and computer screens should be locked when left unattended.
3. If a device is lost, stolen or damaged, it is the User's responsibility to report this security incident as soon as possible to IT staff. The User's responsibility for the activities carried out through their account is limited to the point where they promptly reported any compromise on the account.
4. Refrain from engaging in any activity that might be purposefully harmful to the IT Resources, systems or to any data stored thereon, such as propagating malicious programs, installing unauthorized software, making unauthorized modification to data or using any program or command in a manner that can degrade the system performance and/or deny services to authorized Users.
5. Refrain from executing any form of network and security monitoring or scanning, unless required by their job role.
6. Refrain from changing the configuration or attempting to circumvent or subvert security measures on operating systems and software unless this activity is a part of their normal job/duty.
7. Refrain from making copies of any the Town's software, files, applications or utilities for use outside the Town.
8. Refrain from using IT Resources and other resources in such a way so as to incur lawsuits or other liability against the Town (e.g., by violating copyright laws, creating and distributing false financial data, making defamatory allegations, etc.).
9. Refrain from using IT Resources or other resources to gain unauthorized access to the Town's resources or the resources of other companies or entities (e.g., government, business partners, vendors, etc.).
10. Ensure that they save any crucial business related data on Town provided/approved server drives.
11. IT staff provide services in Town facilities only.
12. Users must reimburse the Town for any personal expenses incurred on any IT resource. This includes apps purchased or long distance personal expenses incurred on a SmartPhone or tablet computer.

13. When travelling to another country with a Town SmartPhone, it is the User's responsibility to ensure that IT staff is notified, and a travel package is purchased for the appropriate country before leaving Canada. Otherwise, the User will be personally responsible for any expenses.

Ownership of Information and MFIPPA

1. The Town is subject to MFIPPA. As such, the public has rights to access certain information under the care and control of the Town. All information on the IT Resources will, by default, be owned by the Town and deemed under the Town's care and control.
2. The use and disclosure of Electronic Messaging shall be covered under the provisions of MFIPPA and as such is subject to the provisions in the Records and Information Management Policy, POL.COR.22.01. Electronic Messages sent to or received from a User's Town email address shall be considered machine-readable records owned by the Town, for the purposes of MFIPPA, and as such will be considered electronic records. **Because email messages are considered Town records, they should NEVER be permanently deleted.** Moving messages to the Deleted items folder or moving them to folders the User creates within their mailbox are acceptable methods of organizing work, but permanently deleting any message is not allowed. This includes any messages that are personal in nature.
3. The Town retains ownership in and shall have exclusive control over the reproduction of Electronic Messages.
4. 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, SmartPhones 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 Director must be notified.
5. Information considered as private or confidential by MFIPPA must not be posted to a Town website or any other publicly accessible service, unless previously approved by the Town Clerk and Manager IT, and unless the data is protected by appropriate security.
6. Users must not disclose personal or confidential information to persons to whom it may not be disclosed under MFIPPA.
7. For maintenance, audit purposes and investigative purposes (see below for further details of the various investigations), the Town will have access to, and may access, all information stored on the IT Resources.
8. If the Town has grounds to believe a User has contravened or may contravene this Policy, the law, the rights of a third party or their agreement with the Town, the Town will access and review all information contained on the IT Resources.
9. Subject to applicable laws, personal information stored on IT Resources may not be private

and the Town may access same.

Management of Schedule A

HR is responsible to ensure that all Users read and agree to the terms of this Policy before they are permitted to use any IT Resources.

Those Users who do not sign and return the IT Policy Form either on paper or electronically will NOT be assigned any IT resources or be permitted to access the IT Resources, including Electronic Messaging, SmartPhone or computer.

Completed IT Policy Forms (see Schedule A) for Town staff, Library staff, Attainable Housing Corporation staff and Council members are filed with HR.

Completed IT Policy Forms for all others, including volunteers, Attainable Housing Corporation board members, Library Board members and Committee members are filed with the Finance & IT Department.

Executive Director Attainable Housing Corporation is responsible to collect signed IT Policy Forms for Attainable Housing Corporation board members.

Library CEO is responsible to collect signed IT Policy Forms for Library board members.

Management of Contractor Login Accounts

Contractors will not be provided with logins to Town IT Resources; IT staff will attend all online sessions with contractors where elevated security is required. The Manager IT may approve exceptions to this rule on a case by case basis.

Users are requested to include IT staff throughout the project when dealing with Contractors who need access to Town IT Resources.

Non-Disclosure Agreements for Contractors

If a Contractor requires access to Town IT Resources, the Contractor is required to sign a Non-Disclosure Agreement (NDA). The Manager in charge of the project is responsible for ensuring the NDA is signed by the Contractor and that the form is delivered to the Finance & IT Department for storage.

Access to Absent Staff Files and Messages

From time to time there is a requirement for IT staff to provide temporary access to staff in other Divisions when an employee is out of the office for any reason. IT staff have the authority to provide access to both mailboxes and I: drive files under the following conditions:

a. Requests can be made by the absent employee's Manager, Director or Administrative Assistant
b. Approval must be provided by the Department Director, the Manager HR or the CAO (or designate)

c. Access to the data can be granted to whoever the requestor designates, as long as the approver is aware.

Requests and approvals must be provided by email or on the IT help desk.

Access will be provided for a maximum period of 2 weeks, at which point approval must be received again.

Access to Town Devices while on a Leave

In coordination with the IT Onboarding/Offboarding Users Policy, POL.ADM.21.02, staff who are on an extended leave for more than 7 days will be asked to surrender all Town devices, such as mobile phones and laptops, to HR.

Texting on Town Phones

Due to its transient nature, texting for business purposes is NOT recommended. Also note that a text message is a record owned by the Town. It is difficult to search devices for text messages, but regardless, IT could be asked to search a Town phone for investigative purposes, as outlined in the Investigations section of this Policy. When doing investigations to search texts on phones, note that all texts will be searched, including personal ones. It is recommended that staff use Microsoft Teams chat for business related messages, which is available to all Users and is also searchable for investigative purposes, in place of texting.

Personal texting on a Town phone is permitted, though should be limited just like any other personal use of Town IT Resources, as outlined in the Internet and Electronic Messaging Use section of this Policy.

Forward Facing Corporate Service Accounts

Forward facing corporate service accounts are those that are created at a vendor website that are for services provided by the Town to the public. For example, this could be a website that provides mail distribution services (SurveyMonkey, MailChimp, CyberImpact, Canva, etc.) or for social media sites.

Always use generic mail distribution addresses containing multiple staff members to sign up for these services.

Passwords for forward facing corporate service accounts must be created by and stored in IT.

Investigations

1. Town IT staff have the authority to do targeted searches on any IT Resources including:
    - Electronic Messaging mailboxes
    - Files on the Town's IT resources
    - Social media sites

- Microsoft Teams chat
- Phone systems
- Text messages
- Internet usage

under the following situations and with the following authorizations. Searches will take place without the notification of the User(s) affected. Requests and approvals must be provided by email or on the IT help desk. Any of the above mentioned searches may be performed by IT staff or an external agency under the Manager IT's direction.

a) MFIPPA requests

   i. Requests can be made by the Director Legal Services or designate
   ii. No further approval is required

b) MFIPPA requests from the Library

   i. Requests can be made by the Library CEO or designate
   ii. Approval must be provided by the Manager HR or the CAO (or designate)

c) MFIPPA requests from the AHC

   i. Requests can be made by the AHC Executive Director or the AHC Board Chair/Designate
   ii. Approval must be provided by the Manager HR or the CAO (or designate)

d) File and Document Management System Searches

   i. Requests can be made by the Department Director
   ii. No further approval is required

e) Town legal case

   i. Requests can be made by the Manager Purchasing & Risk Management, the Director Legal Services or designate
   ii. Approval must be provided by Manager HR or the CAO (or designate)

f) Abuse of Town computer systems by Town Staff or a member of the Public

   i. Requests can be made by the Department Director or the CAO (or designate)
   ii. Approval must be provided by the Manager HR or the CAO (or designate)

g) Abuse of Town computer systems by Library staff or Library board members

   iii. Requests can be made by the Library CEO or the Library Board Chair/Designate
   iv. Approval must be provided by the Manager HR or the CAO (or designate)

h) Abuse of Town computer systems by AHC staff or AHC board members

   v. Requests can be made by the AHC Executive Director or the AHC Board Chair/Designate
   vi. Approval must be provided by the Manager HR or the CAO (or designate)

i) Abuse of Town computer systems by a member of Council

i. If anyone has reason to believe that a Council member has abused Town computer systems a complaint may be submitted to the Clerks Department in written form. This complaint will be forwarded within 48 business hours to the Town's Integrity Commissioner who will process it in accordance with Section 223.3 of the Municipal Act, 2001
ii. As part of the investigation process, the Integrity Commissioner may request and direct the types of system searches, as outlined above

j) From time to time, IT staff perform internet usage statistic reporting and network security audits.

2. Details of any investigation above, 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 Director of the individual in question in consultation with HR, to determine if disciplinary action is required.

Exclusions

The following User groups are not covered by this Policy:

1. Public network Users
2. Contractors and business partners providing IT services in Town facilities who use the corporate network

References and Related Policies

POL.COR.18.10 Social Media Policy

POL.COR.22.01 Records and Information Management Policy

POL.ADM.21.02 IT Onboarding/Offboarding Users Policy

POL.HS.10.12 Workplace Violence and Harassment Policy

POL.COR.07.07 Code of Conduct for Members of Council

POL.COR.13.24 Progressive Discipline Policy

Consequences of Non-Compliance

Compliance to this Information Technology Acceptable Use Policy is mandatory for all Users accessing the Town's IT Resources. Violations of this policy may result in disciplinary action up to and including termination of employment, per POL.COR.13.24 Progressive Discipline Policy.

Any exception to the Policy needs to go through a formal exception management process.

Review Cycle

This policy will be reviewed every two years by the Manager Information Technology and the Senior Management Team.

Schedule A - February 24, 2020 Version

Information Technology Acceptable Use Policy Agreement Form

I 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: **Type your name here**

Date: **Select today's date here**

Note: please save and email this form to Cathy Bailey (cbailey@thebluemountains.ca) to confirm your agreement to follow and abide by the terms of this Policy. The email and this form will be placed in your employee file in HR.