

NO: HR-3

Title: Code of Conduct



Type: Human Resources

Authority: Board

Resolution No: BMPL 2018-77 on 4-19-18; POL-ADM.2018.25

Associated Documents: Ontario Employment Standards Act, SO 2000, c.41

Purpose

This Code of Conduct provides a standard to guide conduct of Personnel in all matters related to the Library.

Scope

This policy refers to all class of Personnel as identified in HR1 General.

HR3.1 Expectations

1. All Personnel are expected to behave in a manner which is professional, and which upholds the standards of safety and respect for users.
2. All Personnel shall behave in accordance with the POL-PUB.2018.66 *Rights and Responsibilities of Users* and all policies which refer to conduct, including the Corrective Action Procedures and Termination and Severance of Employees.
3. Infractions shall be addressed by the direct supervisor and/or CEO according to the Corrective Action Policy.

HR3.2 Responsibility to BMPL and Co-Workers

1. All Personnel are responsible for:
 - 1.1. Conducting the business affairs of the BMPL in good faith, and with honesty, integrity, due diligence, and competence.
 - 1.2. Serving the public with respect and dignity.
 - 1.3. Protecting privacy and confidentiality except as otherwise required by law or as authorized by the CEO. No personnel will share, copy, reproduce, transmit, divulge or otherwise disclose any confidential information related to the BMPL, including but not limited to user information.
 - 1.4. Refraining from use of any form of public negative promotion or defamation of the library, museum, gallery, its Board, CEO, other employees, Personnel, or services. Negative promotion includes, but is not limited to, verbal interactions, personal social/electronic media posts, written formats, audio/video, and publications. Negative communications to any member of the public through any medium shall not be tolerated and may be grounds for dismissal.
2. All Personnel must sign and abide by the *Code of Conduct* and *Oath of Confidentiality*. These agreements endure in the event of termination from the Blue Mountain Public Library. Whistle Blower legislation is not deemed a breach of confidentiality, as long as the confidential information is reported to the appropriate body.

HR3.3 Acceptable Use of Property

The BMPL property, technology, hardware and software, intellectual property and materials available to Personnel are provided for the purpose of conducting the work of the library, museum and gallery and shall be utilized only as authorized, and not for personal use. Information attained during the conduct of the employee's/volunteer's work at the library, museum or gallery must not be used for personal purposes, or prematurely released to any member of the public without explicit permission from the CEO.

Original Approval: 4-19-18
Amended On: _____

POL-ADM.2018.72 Title: *Operational Technology Use*



Type: Administrative
Authority: CEO
Approval Date: 5-22-18
Associated Documents: FAF.18.80 IT Acceptable Use Policy

Section 1 The Blue Mountains Public Library’s Website

The BMPL personnel all agree to follow the Town IT policies when using networked systems.

Section 2 The Blue Mountains Public Library’s Website

1. The Blue Mountains Public Library will maintain a website that provides:
 - 1.1. Information about services and operations;
 - 1.2. Access to the catalogue;
 - 1.3. Access to online museum collections and archives
 - 1.4. Access to subscription databases, streaming and download services, ebooks and digital audiobooks;
 - 1.5. Selected, evaluated, and organized collection of reliable and current information sources available on the Internet.
2. The employees should conduct due diligence when linking to the website, however employees are only responsible for the content of website/social media managed by BMPL, and not the content of outside resources or links.
3. The CEO shall ensure the BMPL is searchable with its own Domain Name System (DNS).

Section 3 Compliance

1. The CEO will ensure that all personnel working in the buildings are informed and familiar with this policy, the Acceptable Use Rules, and the Internet Use Statement.
2. The staff will make all reasonable efforts to ensure that all users comply with the Acceptable Use Rules and the Internet Use Statement.
3. Actions taken by staff may be appealed to the CEO. The CEO’s decision is final.
4. The CEO will support staff in fair and informed enforcement of this policy and associated rules.

Section 4 Maintenance and Security

1. The CEO will maintain a Technology Plan which will be reviewed and endorsed by the Board at least every four years.
2. The CEO will ensure access is provided to software, products, and operating systems for use by the staff and/or patrons and as available within the current budgetary constraints.
3. The CEO will ensure that all security measures are in place, including but not limited to:
 - 3.1. Password protection of secure sites;
 - 3.2. Active virus software on all workstations;
 - 3.3. Server redundancies such as firewalls that are active and in place;
 - 3.4. Automated or dual drive back-up of server and protocols;
 - 3.5. Emergency power back-up and shut down mechanisms for server and workstations.

4. The BMPL, in partnership with the Town, will maintain all technology so that it is in good working order for Patrons and Staff.
5. The BMPL will ensure security protocols are in place to protect the physical infrastructure including smoke/fire detectors and insurance. Video surveillance, entry alarms, heat alarms will be included in future capital budgets.
6. Virus and Malware protection shall be on each system to protect the network and files. Public access computers should be used by patrons at their own risk.
7. The BMPL will maintain active licenses for all software housed on workstations and the server.
8. The CEO will conduct a Technology audit of suggested additions annually.
9. The CEO will conduct a Technology inventory semi-annually.

Section 5 Business Continuity and Disaster Protocols

1. The CEO will maintain protocols for business continuity in the event of a technological disaster. A disaster includes, but is not limited to:
 - 1.1. Fire, Flood, or Natural Disaster;
 - 1.2. Theft, Vandalism or Sabotage;
 - 1.3. Server system failure;
 - 1.4. Electrical outages, brownouts, or spikes;
 - 1.5. Life cycle of computers due to age and normal wear;
 - 1.6. Data corruption or loss due to Virus, Worm or Trojan;
 - 1.7. Patron database and ILS corruption or loss.
2. To maximize business continuity the CEO and Board will:
 - 2.1. Maintain insurance policies;
 - 2.2. Employee redundancies of drives and server backups;
 - 2.3. Utilize UPS, surge protectors and other electrical redundancies;
 - 2.4. Plan for lifecycle of systems and for ongoing maintenance and replacement;
 - 2.5. House internet and intranet firewalls and security software;
 - 2.6. Employ an ILS where daily backup of information and redundancy drives are guaranteed.
3. The CEO will maintain an up-to-date Succession Manual, Staff Manual, and IT procedures/passcodes in the event of death, termination, or some other reason why the CEO, IT, or other protocol and passcode holder cannot provide information for succession. The CEO will inform the Manager of Technical & Virtual Services on an ongoing basis where these materials can be found and ensure that Business Continuity is not hampered by lack of succession information.

Section 6 Responsibility and Access to Technology

1. The CEO will provide a master list of passwords for the Library in the confidential section of the succession manual.
2. The CEO will be responsible for requesting access points for staff, volunteers and members of the Board for e-mail accounts, staff login, and other access points. These will be at the CEO's discretion and be determined by the needs of each position.
 - 2.1. All staff will have access to staff accounts and have access to complete basic patron demands such as waive fees, reset patron passwords, override basic functions of the system;

- 2.2. Volunteers may have access to accounts but be logged on by staff;
- 2.3. One designated staff will have access to the CEO desk and personal files when the CEO is away from the building for long periods such as trips, illness, or vacation. All requests for information when the CEO is away but returning in 48 hours or less can be held until the CEO's return;
- 2.4. A comprehensive list of password needed by Staff will be maintained within Z:\Technology - Computer_Help A03.

Section 7 Personnel Use of Technology

1. All personnel who have access to library technology will use said technology for work purposes.
2. Cell phones which are provided shall be used only for work business. Personal calls are not permitted.
3. Malware and viruses can be passed to networked systems even when protective software is in place. The best line of defense is the personnel who open files with care and caution.
4. Laptops, tablets, and PCs shall be used by staff for Library, Museum and Gallery work only. No personal activities may occur off hours or off site without CEO permission.

Original Approval: 5-22-18
Amended On: _____



Policy and Procedures

POL.COR.12.13

Information Technology Acceptable Use Policy

Policy Type:	Corporate Policy (Approved by Council)
Date Approved:	June 4, 2018
Department:	Finance and IT Services
Staff Report:	FIT.12.17, FIT.14.47, FAF.17.54 and FAF.18.80
Date Revised:	June 4, 2018
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.

"User" means any person who interacts directly or indirectly 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") who use Town IT Resources.

Definitions

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

“CEO” means the Chief Executive Office of the Library.

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

“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.

“Electronic Messaging” includes all forms of messaging, including the traditional Town Email system, instant messaging applications like Skype and social media forums like Twitter, YouTube, Instagram and Facebook.

“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 and Wide Area Network and all connected components, e.g., routers, switches, servers, hosts, storage devices, PCs, Mobile Devices (including cell phones and smart phones), 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.
- Information hosted on the foregoing

IT Resources excludes equipment and software installed on the public network at the Library.

“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, Blackberry’s and other smart phones.

“Portable Storage Device” 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, DVDs and floppy disks.

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

“User” means employees, volunteers and elected officials.

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. Sharing passwords is prohibited, unless using a group email account or when requested by IT staff. Passwords should only be shared verbally and only to IT.
2. Users are responsible for all activities carried out with their User ID.
3. Users must not access IT Resources by using the User ID and password of any other User.
4. 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.
5. 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).

6. 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, with the exception of remote email services (Outlook Web Access) and any future remote work from home systems.

Information Confidentiality

1. Users must delete all Town data from their Portable Storage Devices as well as Mobile Devices, both Town provided and personal, before discarding or handing the device over to any person or entity unless it is subject to an internal Town investigation or requested by a law enforcement agency.
2. Users must exercise due diligence, as they 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 are accountable for their actions on the Internet and Electronic Messaging systems.
2. 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.
3. Users must not use Town Internet or Electronic Messaging to gamble, make personal gains or conduct personal business.
4. Users must not make official commitments through the Town Internet or Electronic Messaging on behalf of the Town unless authorized to do so.

5. Users must not download copyrighted material such as music files, video files or other large files unless they are specifically related to their job.
6. 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.
7. Users must always use Town email addresses for Town communication. Users must not use any personal email addresses to send business related communications.
8. Users must not post, download or upload on the Internet or forward Electronic Messages containing Inappropriate Material. Users must delete such Electronic Messages immediately.
9. 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.
10. Users must not use the IT Resources to send unsolicited messages (spam) to any internal or external address.
11. Users must not use the IT Resources, Electronic Messaging or other communication channels to:
 - a. embarrass or discredit the Town, our employees, officials or the persons with which we do 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.
12. 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.
13. Use of the network, Electronic Messaging, Internet or any IT device for any purpose related to a user's commercial business is not allowed.

14. Limited, occasional or incidental use of the network, Electronic Messaging, 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.
15. 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.
16. 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.
17. Messages posted to Social Media web sites must conform to all Town standards, policies and regulations, including this policy.
18. 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).
19. 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.
20. The Town reserves the right to blacklist or block any Internet site that it deems to be inappropriate or which may affect network or user performance.

Use of IT Resources

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

Information Technology Acceptable Use Policy

1. Connect/deploy only Town provided/approved IT Resources 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, smart phones must remain in a protective case and devices must not be left in unattended vehicles.
3. 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 authorised Users;
4. Refrain from executing any form of network and security monitoring or scanning, unless required by their job role;
5. 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 your normal job/duty;
6. Refrain from making copies of any the Town's software, applications or utilities for use outside the Town;
7. 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.);
8. 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.);
9. Ensure that they save any crucial business related data on Town provided/approved shared storage drives.
10. IT staff provide services in Town facilities only.

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. Electronic 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 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, 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.
5. 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 the Town Clerk and Manager Information Technology, 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. The use and disclosure of Electronic Messages shall be covered under the provisions of MFIPPA.
8. Electronic 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.
9. 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 the Town Clerk and Manager Information Technology.
10. 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.
11. 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.
12. Subject to applicable laws, personal information may not be private and the Town may access same.

Investigations

1. Town IT staff have the authority to do targeted searches on Electronic Messaging mailboxes, server files and internet usage under the following situations and with the following authorizations. Searches will take place without the notification of the user(s) affected. All approvals must be in writing or by email.
 - a. MFIPPA requests
 - i. Searches may include Electronic Messages and files on all servers
 - ii. Requests can be made by the Town Clerk or Deputy Clerk
 - iii. No further approval is required
 - b. MFIPPA requests from the Library
 - i. Searches may include Electronic Messages and files on the Library server
 - ii. Requests can be made by the Library CEO or designate
 - iii. Approval must be provided by the Manager HR or the CAO
 - c. File Searches
 - i. Searches may include files on Departmental and Corporate Drives
 - ii. Requests can be made by the Department Head
 - iii. No further approval is required
 - d. Town legal case
 - i. Searches may include Electronic Messages and files on all servers
 - ii. Requests can be made by the Manager Purchasing and Risk Management, the Town Clerk or another legal entity
 - iii. Approval must be provided by Manager HR or the CAO
 - e. Abuse of Town computer systems by Town Staff
 - i. Searches may include internet usage, Electronic Messages and files on all servers
 - ii. Requests can be made by the Department Head or the CAO
 - iii. Approval must be provided by the Manager HR or the CAO
 - iv. Searches may be performed by an external agency
 - f. Abuse of Town computer systems by Library staff
 - i. Searches may include internet usage, Electronic Messages and files on all servers
 - ii. Requests can be made by the Library CEO or the Library Board Chair/Designate
 - iii. Approval must be provided by the Manager HR or the CAO
 - g. Abuse of Town computer systems by Council
 - i. Searches may include internet usage, Electronic Messages and files on all servers
 - ii. 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
- iii. As part of the investigation process, the Integrity Commissioner may request and direct the types of system searches, as outlined above
 - iv. At the Integrity Commissioner's direction, searches may be performed by an external agency
- h. 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 Head of the individual in question in consultation with Human Resources, to determine if disciplinary action is required.

Monitoring

The Town reserves the right to monitor activities undertaken on its IT Resources.

Exclusions

The following user groups are not covered by this Policy:

1. Public network users
2. 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

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

Consequences of Non-Compliance

Compliance to this Information Technology Acceptable Use Policy is mandatory for all Users accessing the Town's IT Resources. Breaches to the Policy, where identified, will be investigated and then the action pertaining to either the Town's disciplinary and/or contractual procedures may be applied, including and up to termination.

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

The Information Technology 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 Resources. Those Users who do not sign and return the IT Policy Form will NOT be assigned any IT resources or be permitted to

access the IT Resources, including Electronic Messages, BlackBerry smart phones or computer. Completed IT Policy Forms (see Schedule A) for Users are to be filed with Human Resources.

Any personal expenses incurred on any IT resource must be reimbursed to the Town by the User. This includes apps purchased or expenses incurred on a BlackBerry or tablet computer.

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: _____