The Corporation of the Municipality of Brockton

By-Law 2019-125

Being a By-Law to Adopt an Amended Information Technology Acceptable Use Policy for the Municipality of Brockton.

Whereas The Council for The Corporation of the Municipality of Brockton deems it expedient to establish policies;

And Whereas the *Municipal Act 2001, S.O. 2001*, c 25, Section 5(3), as amended provides that a municipal power, including a municipality's capacity rights, powers and privileges under section 9, shall be exercised by by-law;

Now Therefore the Council of The Corporation of the Municipality of Brockton enacts as follows:

1.0 That The Corporation of the Municipality of Brockton Council hereby adopts an Amended Information Technology Acceptable Use Policy as contained in the attached Schedule "A" to this By-Law.

2.0 That By-Law 2012-02 is hereby rescinded.

3.0 This By-Law shall come into full force and effect upon final passage.

4.0 This By-Law may be cited as the "Adopt Amended Information Technology Acceptable Use Policy By-Law".

Read, Enacted, Signed and Sealed this 15th day of October, 2019.

_____ _____

Mayor – Chris Peabody Clerk – Fiona Hamilton

Brockton
Come home to community

Policy A23-0100-12

Information Technology and Acceptable Use Policy

Department:	All Departments and Council	**Policy Number:**	H02-0600-19
Section:	Administration	**Effective Date:**	January 9, 2012
Subject:	Information Technology	**Revised Date:**	October 15, 2019
Authority:	By-Law 2012-02, By-Law 2019-125		

1. Purpose

The purpose of this policy is to ensure that users of the Municipality of Brockton information technology assets and services do so in a manner that supports municipal programs services and activities; protects preserves and avoids waste of these resources; maintains the appearance and substance of the Municipality's good public reputation and complies with laws and regulations.

2. Application

This policy applies to all Municipal employees, Municipal Councilors non Municipal employees and/or contractors, as well as clients who are authorized to use Municipal computers and related equipment, software and programs by the Information Technology Coordinator at the request of the relevant Department Head. (Hereafter referred to as users)

The Chief Financial Officer (CFO) will identify responsibilities and requirements of all technology users and provide guidance for the use of municipal desktop personal computers, laptops, and related components, technologies and supporting software and hardware.

The Municipality of Brockton regards all of its system hardware, software, information, and communications facilities as assets of the Municipality. These assets require protection from deliberate or accidental misuse, disclosure and liability resulting from negligent use. Use of these systems is a privilege, not a right, which carries significant Municipal and personal responsibility.

Users of the Municipality's resources are to use those resources for activities that are their functional responsibility and support the Municipality's business. Other uses, such as for personal gain, or entertainment are prohibited.

Users are to apply computer resources in a manner that improves efficiency and effectiveness in accomplishing their tasks that are to the net benefit of the Municipality. Users will also be responsible when called upon for documenting and communicating benefits realized through improvements made to Departmental and/or Municipal computer resources.

Users of the Municipality's computer resources have the responsibility to understand the terms of the Information and Technology Acceptable Use Policy. Violation of the policies may result in disciplinary action, deemed necessary by the Municipality. Questions regarding the

application of these policies should be directed to Department Heads or the CFO who oversee Information Technology within the Municipality of Brockton.

3. Procedure

Overall Principles:

3.1 All equipment and software programs, information and data installed or created on Municipal equipment belong to the Municipality of Brockton. This includes all programs, document, spreadsheets, databases, and methods or technologies developed using Municipal equipment and/or software, while employed by the Municipality.

3.2. Information or data cannot be copied to removable media (e.g. portable drive, external drive, or writeable CD) or downloaded electronically to another individual, agency, public or private, for any purpose other than approved Municipal business. Should a user have any doubt about the appropriateness of a request for information, they must obtain the advice of the applicable Department Head and the CFO.

3.3 All electronic documents related to the Municipality, including emails that are created, received and retained by a user either electronically or on paper, are considered to be records of the Municipality and as such are subject to all of the access and privacy provisions of the Municipal Freedom of Information and Privacy Act and the Municipal Records Retention Program Policy.

3.4. Equipment and software cannot be used for any activity for which a user receives remuneration or "in-kind" service or other personal benefits other than those received directly from the Municipality

3.5. Incidental and occasional personal use of Municipal equipment and software is allowed, similar to occasional use of the Municipality's telephones, providing such limited use will not result in any measurable expense to the Municipality in time or materials. However, such use is subject to limitations of this policy.

3.6 Use of Municipal electronic systems including but not limited to equipment hardware, software, data, databases, internet resources (hereafter "electronic systems") is intended to be used primarily for business purposes. Municipal electronic systems are not intended for personal use and users (including council members) shall not have any expectation of privacy when using any Municipal electronic system. The use of a Cell Phone/Mobile device for personal use within reasonable limits is permitted as long so long as it does not interfere with or conflict with business use, and does not impair the employee's ability to fulfill their work duties.

3.7. All employees have a responsibility to report a suspected policy violation to their Department Head who in turn will report same to the CAO. It will be at the discretion of the CAO on how the violation is processed. Council members have a responsibility to report any suspected violation directly to the CAO.

3.8 Monitoring and reporting of abuses of this policy will not distinguish between business and personal use.

3.9 At its discretion, the Municipality through the CFO and at the direction of the CAO may access, monitor, (including random spot checks) review, copy or disclose any electronic communications made in any way at any time by a user.

3.10 The Department head is responsible for obtaining a signed Information Technology Acceptable Use Policy Acknowledgement from each employee for whom a personnel record is maintained and has access to Municipal technology equipment. The Clerk is responsible for obtaining a signed Information Technology Acceptable Use Policy Acknowledgement from each member of Council .This signed form shall be kept in the relevant personnel file.

4. Internet Access and Acceptable Use

4.1 lnternet access is provided to users for research and communication purposes relevant to the Municipality's business and to provide such information to residents and business partners.

4.2. Department Heads, at their discretion and with the assistance of the CFO may choose to block public Internet access for specific employees and/or locations.

4.3 Municipal-provided Internet access and email are Municipal resources and are to be used for Municipal business purposes.

4.4 Personal use of the Internet and email is authorized within reasonable limits as long as it does not interfere with or conflict with business use, does not impair the employee's ability to fulfill their other work duties and provided the employee has their supervisor's approval. However, under no condition is the Internet to be used to access sites that generally are viewed as inappropriate.

4.5 Employees and Council members and all users shall not knowingly:

4.5.1 Visit Internet sites that contain obscene, pornographic, hateful or otherwise objectionable content.

4.5.2 Send or willingly receive any material that is or can be perceived as obscene or defamatory or which is intended to annoy, harass or intimidate another person or group of persons.

4.5.3 Use continuous access technology such as "Push or Pull" common to many news services, or other websites that do not require user intervention to refresh information (e.g. Real Player, Limewire, iTunes)

4.5.4 Use the Internet for illegal or unethical purposes, or to gather information to support illegal activities.

4.5.5 Send or forward chain letters or excessive quantities of email or spam; or indiscriminately copy large e-mail messages to individuals.

4.5.6 Distribute a virus or other harmful component.

4.5.7 Violate copyright laws by unlawfully downloading or using information or software that is protected by copyright.

4.5.8 Disclose confidential information about the Municipality or its customers.

4.5.9 Express opinions that appear to be on behalf of or representing the Municipality.

4.5.10 Make negative or harassing comments about individuals, employees or the Municipality in chat rooms, blogs, Facebook, My Space etc.

4.6 Downloading of non-executable files for business use is permitted. These would include reports, Adobe "PDF" files, spreadsheets, etc. Users must ensure the source is reliable as viruses can be introduced to the system through spreadsheets and other documents.

4.7 Executable files (Programs) may not be downloaded without authorization from the CFO. Such software, if approved, must be checked for viruses before execution by the CFO. No user will attempt to download unauthorized software or to alter network configurations.

4.8 Department Heads are responsible for their respective employees' use of the Internet. The Department Head along with the CAO, will co-ordinate any action as a result of abuse of Internet privileges.

4.9 If email is not required as a permanent record of the Municipality, it shall be read and deleted from the system. If email is to be retained, employees shall print a paper copy and place it in an appropriate file and then delete the email. Alternatively, an electronic copy can be retained in an electronic folder.

4.10. If email is forwarded to external service providers, the content is then no longer under Municipal control. Such email cannot be retracted or deleted by the sender. Users who use this feature must use caution to ensure that the external service provider respects the confidentiality of their email.

4.11 Email messages are like any other communications that are created to correspond with customers. As a result, professional business practices shall be adhered to in respect to the creation and content of email messages.

4.12 The Internet provides a variety of web-based social and personal networking tools that the Municipality may find useful and appropriate to disseminate or share information with staff and the public. These include sites such as Facebook and My Space and services such Blogs, Twitter, Tweet deck, Hootsuite or Linked In. Professional business practices shall be adhered to in respect to the creation and content of these web based services and must have the permission of the department head and the IT Coordinator. (Refer to

specific Social Media Policy).

5. Software Licenses, Acquisition, Installation and Support

5.1 Only software provided by the Municipality and/or licensed to the Municipality may be installed on computer hardware that is provided by the Municipality. Unauthorized software shall not be used. Any exceptions to the above require the authorization of the Department Head and approval from the CFO.

5.2 Software shall not be copied except for the sole purpose of backup. Piracy is strictly prohibited.

5.3 All software and hardware must be approved, purchased, installed and supported by the Information Technology staff. Some exceptions may be made but are not encouraged for the departmental purchase of hardware that operates separately from the Municipal network. These purchases must be approved by the CAO with consultation with the IT staff and once approved purchases must be logged and inventoried by the IT staff. Department Heads must not expect support from the IT Staff for such purchases.

5.5 The CFO will retain licenses and original copies of all licensed software.

5.6 Internet downloads (including software upgrades, freeware and shareware) must not be installed without approval from the IT Co-ordinator.

5.7 The Information Technology Staff is responsible for assisting departments, upon request, with searching for software that best fits their business needs. Departments may also search for their own business software, however the CFO will approve the department's heads selection of software to ensure that the choice is not in conflict with Municipal electronic systems (approved software for the Brockton network).

5.8. Departments may request that a product be added to the Municipal electronic system with support provided by the Information Technology Staff. The CFO will add that product to the list of acceptable software where, in its judgment, the product will be of interest and benefit to a substantial number of Municipal users. All such requests shall be made to the CFO and approved by the CAO.

5.9 The CFO has the ability to detect all software installed and utilized on computers throughout the Municipality. This capability will be used to monitor and ensure compliance with this policy.

6. Management of Users

6.1 Department Heads must notify the CFO, who will be responsible for all changes to be made to employees' User Ids. This includes disabling the person's access (temporarily or permanently), deleting the User ID, adding new users, changing access rights, advising of employee location changes, etc.

6.2 Department Heads will provide CFO with a list of staff who have been transferred,

terminated or newly employed. These lists will be used to verify Information Technology records on a random basis.

6.3 Upon employee termination or transfer, (or when a council member is no longer in office) all documentation, email, programs. etc. are to be turned over to the employee's Department Head or in case of Council to the Clerk . No information is to be deleted or otherwise made inaccessible or non-functional regardless of storage medium. All information remains the property of the Municipality.

6.4 Users must surrender any documentation in their possession relating to the Municipality's hardware or software upon termination of their employment.

6.5 Authorization must be given by the department head in conjunction with the CAO for an employee to have computer access (laptop, touch pad) outside the municipality or in their home or for after-hours remote access to computers. All setup arrangements will be channelled through the CFO. Upon issuance of the device, staff must complete and return to the CFO, the Laptop Use Borrower Agreement Appendix "B".

6.6 Council laptops (or touch pad devices) are issued at the beginning of each Council term and all council members must comply with the requirements of this policy. Upon issuance of the device, Council must complete and return to the CFO, the Laptop Use Borrower Agreement Appendix "B".

6.8 CFO provides storage for individual files on designated drives throughout the network. No new drives or changes are made without the authorization of the CFO.

6.9 All User IDs and passwords are confidential to each user and are not to be shared amongst users unless CFO or Department Head authorization is given.

6.10 Users are accountable for all activities that occur under their User ID/password. Users are responsible for immediately reporting any known or suspected compromise of their User ID/password. If an irregularity is suspected, CFO can examine logs to determine if unauthorized usage may be occurring.

6.11 Passwords:

6.11.1 Passwords must not be left where someone else can find it (e.g. taped to a PC, under a keyboard, etc).

6.11.2 All users are responsible for changing their passwords at least once every 60 days. Passwords shall be easy for the user to remember but difficult for others to determine.

6.11.3 Employees should not select the option to "Remember this password" when asked. This provides access to documents to anyone who may be using the employee's computer.

6.11.4 Minimum password length is 12 characters, may not contain your username or any part of your full name and must contain characters from 3 of the following categories:

- Uppercase letters
- Lowercase letters
- 0-9
- Special Characters (e.g. !@#$%^&*()_+-=)

6.11.5 Password changes must be given to the CFO immediately upon change for security purposes.

7. Backup and Recovery of Client Data

7.1 The Information Technology Coordinator is responsible for:

7.1.1 Back-up and off-site storage of all software and data maintained on the Municipal server on a regular basis.

7.1.2 Maintaining adequate backups of municipal programs and applications.

7.1.3 Restoring damaged or lost files from backups maintained for municipal applications and servers.

7.2. Each user is responsible for:

7.2.1 Maintaining backup copies of any documents, data or software stored on local hard drives.

8. Viruses

8.1. The CFO maintains a current version of virus protection software and updates desktop computers with the current virus signatures through the network.

8.2 Employees and council members must not disable the Municipal virus protection software.

8.3. Employees and council members must not distribute files, diskettes, email attachments or other electronic media if you know that the media has a virus.

8.4. The CFO must be contacted immediately if you suspect your computer has a virus. If known, report the source.

9. Policy Violation

9.1 Violation of any part of this policy could result in disciplinary action deemed necessary by the Municipality, up to and including dismissal.

Municipality of Brockton
Information Technology Acceptable Usage Policy Acknowledgment

Surname: _____ First Name _____

Department: _____ Division _____

Telephone: _____ Employee No. _____

Employee Declaration

1. I have read and understand the Information Technology Acceptable Usage Policy.

2. I acknowledge that I am responsible for complying with the Information Technology Acceptable Usage Policy.

_____ _____
Employee Signature Date

_____ _____
Department Head (Please Print) Department Head (Signature)

_____
IT Supervisor (Signature)

Original filed in Employee's Human Resources Personnel File

Municipality of Brockton
Laptop Use Borrower Agreement

Surname: _____ First Name _____

Department: _____ Employee No. _____

Laptop Type: _____ Serial Number: _____

Inventory Number: _____ Date: _____

☐ Mouse Provided ☐ Power Cord ☐ Carrying Case

Declaration

By my signature below, I agree to all the following statements:

1. I have read, understand and accept the above conditions
2. If a laptop is lost or significantly damaged, I will be responsible for reimbursing the municipality for the repair or replacement of the system. Replacement cost for the laptop computer is based on the purchase price of equipment with similar specifications. Repair costs will be based on actual costs of parts and labour.
3. I will return the laptop at the end of my council term or employment with the Municipality
4. I will not add, delete, or alter computer hardware, software, or settings.

_____ _____
Employee/Council Signature Date

_____ _____
Department Head (Please Print) Department Head (Signature)

_____
IT Supervisor (Signature)

Original filed in Employee's Human Resources Personnel File