MUNICIPALITY OF PORT HOPE
RESOLUTION

Date: 20 September 2022

54/2022

MOVED BY: _____

SECONDED BY: _____

WHEREAS Council at the Committee of the Whole meeting held on September 6, 2022 considered Staff Report CS-15-22 regarding Acceptable Use of IT Assets Policy;

NOW THEREFORE BE IT RESOLVED THAT Council adopt the Acceptable Use of IT Assets Policy attached hereto.

_____
Mayor Bob Sanderson

Information Technology Policy		Effective:	September 20, 2022
		Approved:	September 20, 2022
Policy:	**Acceptable Use of IT Assets Policy**	By-law:	n/a
Section:	IT Policies	Resolution:	54/2022
Application:	All Users of Municipal IT Systems & Equipment	Supersedes:	6.11, By-law 61/2012

Policy Statement

The Municipality of Port Hope is committed to providing the most efficient, effective, and secure technology environment to the users of its technology services. The Municipality believes that employee productivity and communications are greatly enhanced through the appropriate and effective use of Municipal electronic systems. These systems include, but are not limited to: access to email, files and the internet; productivity software; business applications; and databases.

It is the policy of the Corporation of the Municipality of Port Hope to allow authorized users access to the Municipality's electronic network for authorized uses only.

The Municipality will provide employees with the technology required to carry out their job roles. Each department is responsible for identifying their own technological needs and recommending access levels for staff members. While this policy is as complete as possible, no policy can cover every situation, and thus the user is asked additionally to use sound judgement when using company resources. Questions on what constitutes acceptable use should be directed to the user's supervisor.

Definitions

Technology equipment (Hardware) – a group or "family" of products, which include devices that have a primary function related to the collection, transfer, storage, or processing of electronic data.

Technology services - specialized technology-oriented solutions that combine the processes and functions of software, hardware, networks, telecommunications and electronics and facilitate the use of technology by end users.

Software – a generic term used to describe computer programs or applications.

Data – information processed and stored by a computer or other electronic device.

Network – a group of two or more computers linked together and the associated infrastructure to enable this functionality.

Remote access – the ability to access a computer from a remote location.

User – A person who uses or operates technology equipment on an electronic network (i.e. employees, co-op students, consultants, or contractors).

Objectives

The objectives of this policy are to:

- Explain how technology is provisioned
- Define expectations with respect to the acceptable use of Municipality of Port Hope's technology assets
- Minimize the risk of unacceptable and unlawful use
- Outline the permitted extent of personal use
- Ensure appropriate data security measures are taken
- Provide a guideline for best practices when using email
- Outline expectations of landline and cellular telephone usage
- Communicate the extent of network monitoring

Information Technology issuance and responsibilities

All technology equipment and services shall be acquired through the designated Information Technology (IT) Administrator in consultation with the IT Coordinator. All Information Technology equipment will remain the property of the Municipality of Port Hope.

The designated IT Administrator will be responsible for the support and maintenance of all municipally owned technology assets. Staff experiencing issues with any assets owned by the Municipality should contact the Help Desk for assistance.

Employees are expected to protect the technology equipment in their possession or that they use, and the data stored on it.

Software is to be used for its intended purpose and in accordance with all Municipal policies and by-laws only. It is not to be copied, distributed, installed, or deleted without the appropriate authorization from the designated IT Administrator. All software installed on municipally owned equipment will be legally licensed and authorized for use.

All data collected and stored is to be used for its intended purpose. Data is not to be copied, distributed, edited, appended, or deleted without appropriate authorization.

If a Municipally-owned computer or other technology equipment is damaged, lost, or stolen, the authorized user is responsible for notifying their Manager and the designated IT Administrator immediately so that appropriate action can be taken. If equipment is damaged it needs to be returned to IT for proper repair or disposal.

All technology services, including cloud-based solutions, need to be risk-evaluated by the designated IT Administrator in cooperation with the IT Coordinator to ensure that the provider and solution follow industry standard security and privacy protocols and that municipal information and data is adequately safeguarded.

When Municipally-issued laptops or tablets are taken home, they should be kept in a safe and secure location and not be left unattended in public locations. Laptops and tablets should not be left inside vehicles or in plain sight, however if there are no other options, the device should be secured in the trunk of the vehicle if possible.

Equipment not issued by the Municipality of Port Hope

Computers, laptops, tablets, WiFi Routers, Smartphones, etc. that are not owned by the Municipality of Port Hope are considered unsecure and can introduce security/virus/spyware/threat issues when connected to Municipality of Port Hope's internal network.

Only authorized devices are permitted on the Municipality's network.

Technology from outside vendors or consultants requiring network access needs to be vetted by the designated IT Administrator in consultation with the IT Coordinator before use.

Remote access to the Municipality's electronic network is only permitted via municipally provided devices.

The designated IT Administrator will be responsible for implementing technology that prevents unauthorized devices accessing the network.

Acceptable use

Authorized users are permitted to use the electronic network for the following acceptable and appropriate work activities:

To fulfill work responsibilities and further the Municipality of Port Hope's mission and vision including:

- Researching, accumulating, and disseminating information related to the user's assigned responsibilities;
- Collaborating and communicating with other employees, partners, and clients, according to the user's assigned responsibilities;

- For career development such as conducting professional development activities such as participating in webinars, discussion groups, etc., as they relate to meeting the user's job requirements; and
- Internet access at discretion of department head.

Authorized users should be aware that electronic communications by email are accessible under the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* and may be subject to legal discoveries in the event of litigation.

Any information requested under MFIPPA will be reviewed and exemptions invoked where applicable to protect information such as personal information about employees or clients.

Unacceptable and unlawful use

Unacceptable uses are activities which violate departmental guidelines and/or Municipal policies.

Unacceptable uses include, but are not limited to:

- Accessing, downloading, printing and/or sending any content whose focus is pornography, nudity or sexual acts or that incite hatred against identifiable groups;
- Accessing without authorization, sensitive information (client databases, personal information, etc.);
- Allowing unauthorized users or third parties access to the electronic network;
- Attempting to defeat information technology security features;
- Causing congestion and disruption of the network;
- Downloading unreasonably large files (over 100MB) that may hinder network performance;
- Streaming radio or video for non-business related purposes;
- Remote access of the network with devices not issued by the Municipality;
- Engaging in any activity that could comprise the security of the host servers or computers;
- Engaging in any activity which would in any way bring discredit, disrepute or litigation upon the Municipality;
- Making public criticisms of Municipality of Port Hope or other government policy(ies);
- Representing personal opinions as those of the Municipality of Port Hope;
- Sending abusive, sexist or racist messages;
- Unauthorized removal or installation of hardware or software;
- Using Municipality's electronic network for private business, personal gain or personal profit;
- Granting another individual access to one's own information technology account by sharing a password;
- Scanning network ports and IP's, packet and email spoofing or any IT security scanning;
- Interfering or denying service to any user or network (i.e. denial of service attack);

- Introducing malicious programs onto any device connected to the Municipal network.

Unlawful uses are activities which include criminal actions that violate the Criminal Code of Canada and those federal/provincial statutes that provide for criminal offences.

For the purpose of this policy, “unlawful uses” is interpreted to include actions that could result in sanctions in a court of law.

If an employee performs an activity in the course of his or her employment over the electronic network, which results in a lawsuit, both the employee and the employer can be held liable.

Unlawful uses of the electronic network include, but are not limited to:

- Destroying, altering, or falsifying data without authorization;
- Infringing on a copyright and unauthorized use of trademarks and patents;
- Intentionally spreading viruses or malware with the intent to cause harm;
- Possessing, downloading, or distributing child pornography;
- Reading or intercepting someone’s electronic mail or other personal information;
- Spreading false allegation or rumours that would insult or harm a person’s reputation;
- Sending messages that contain threats to cause serious bodily harm, damage to personal property or that cause people to fear for their safety or the safety of anyone known to them;
- Sending messages that discriminate against an individual on the basis of: race, national or ethnic origin, colour, religion, age, sexual orientation, marital status, family status, disability and conviction for which a pardon has been granted;
- Various other offences include using, in whole or in part, the electronic network for: fraud, extortion, blackmail, bribery, gambling and dealing in illegal drugs.

If unacceptable, unlawful or unauthorized use of the electronic network occurs, this could result in disciplinary action being taken, from suspension of electronic network privileges, up to and including termination of employment.

Verified egregious acts may result in immediate termination.

Confidentiality

Confidential data must not be:

(A) Shared or disclosed in any manner to non-employees of the Municipality unless authorized by the Director of the department
(B) Should not be posted on the Internet or any publicly accessible systems
(C) Should not be transferred in any insecure manner

Downloading

Downloading of non-executable files for business use is permitted. These include reports (e.g. MS Word or Excel documents), PDF files, information flyers, etc., from other organizations, institutions or government agencies that may be useful to the Municipality.

Executable software (e.g. applications), including files containing embedded executable codes, may not be downloaded. This type of software may be incompatible with other software that the Municipality operates, and/or may contain viruses that could harm the network. If such a file is required, the designated IT Administrator will download and check the file for compatibility and any infection.

If you are unsure of a file or software, submit a ticket to the helpdesk before executing or downloading so IT can verify the source.

Personal use

This policy does allow room for limited and reasonable personal use of the Internet by authorized users. This privilege may be withdrawn at any time by the user's Manager or Director.

Personal use shall be limited to break periods.

Limited and reasonable personal use of Internet access is defined as any personally-conducted online activity or usage for purposes other than those listed in the Acceptable Use section of this policy.

Personal use is limited to the following parameters, and shall not:

- Add to costs or network overhead;
- Be for financial gain;
- Compromise the integrity and security of the Municipality's electronic network;
- Conflict with any other existing policy or practice;
- Have a negative impact on user productivity or efficiency;
- Interfere with the conduct of normal municipal business;
- Use bandwidth draining applications such as excessive internet radio or video streaming;
- Involve the downloading of any type of media or program to the Municipality's network.

Social networking sites

The use of social networking sites (Facebook, Twitter, etc.) and blogs are subject to the same limitations of the Acceptable Use and Personal Use section of this policy.

Employees that use these sites are prohibited from publishing any private organizational information therein, or any negative comments regarding the Municipality and/or employees.

Telephony

The Municipality provides local landline telephone services to all employees that require them to carry out their duties.

When making or receiving private telephone calls staff should take account of the following regulations:

- The making/receiving of private telephone calls should be kept to a minimum and be of short duration
- Long distance calls incur charges and shall not be made for personal use outside of emergency situations
- Private telephone calls should be timed whenever possible to ensure minimum disruption both to the work of the individual and to the workload of colleagues
- It is not acceptable for staff to conduct regular, private business or administration using the Municipality's telephone network. Any such abuse of the telephone system could result in the instances being considered to be of fraudulent nature, which may lead to disciplinary or criminal action
- Such abuse could also result in the withdrawal of the facility to make private telephone calls

The Mobile Device Policy governs the use of cellular phones.

Security

Authorized users are required to take all necessary precautions to prevent unauthorized access to the Municipality's electronic network. For more information regarding security, please refer to the Information Technology Security Policy.

Unattended computers

Users must ensure they do not leave computers unattended while logged on and unlocked.

Employees are obligated to log off or lock their session when they are going to be away from their computer.

Across the corporation, all computer systems are set to lock by default after 15 minutes of inactivity.

Remote network connections will time out after 15 minutes of inactivity requiring the user to reconnect and re-authenticate in order to re-enter company networks.

Data security

All staff handling data (particularly those dealing with personal data) should ensure that the data is secure and that appropriate measures are taken to prevent unauthorized access, disclosure, and loss:

- Municipality of Port Hope issued laptops, tablets and smartphones will be password protected
- Storing electronic data on portable devices such as USB flash drives, portable hard drives, CDs, DVDs, or any computer not owned by Municipality of Port Hope should be avoided. Where this is required, consult the designated IT Administrator to ensure that appropriate controls are put in place.
- If data is transferred to non-municipally owned devices, the data must be strongly encrypted. Consult IT in these situations.
- Confidential data must not be disclosed unlawfully to any third party. Transfers of personal data to third parties must be authorized in writing by the data owner and protected by adequate contractual provisions or data processor agreements, and use safe transport mechanisms.
- Cloud-based file storage solutions (e.g. Dropbox) are not secure and as a result, should not be used.

In certain situations, it is acceptable to use flash or hard drives for transferring non-sensitive content in an unencrypted form. Examples include transferring presentations to non-municipally owned devices via USB stick for the purpose of presenting and sharing content, and using hard-drives for the bulk transfer of other non-sensitive documents and files such as GIS data. For other scenarios consult IT.

In the event of loss of data, report the situation to the Help Desk immediately.

Negligent loss or unauthorized disclosure of personal data, or failure to report such events, may be treated as a disciplinary matter.

Email best practices

Please refer to the Municipality's Email Management Policy.

Remote access

All staff, pending Director and/or Manager approval, may be provided access to connect to the Municipality's internal network using remote access technology for work purposes with an assigned Municipal Device.

Work in this context includes (but is not limited to) web browsing via remote server access, accessing file-based resources, and accessing other Municipal applications.

As remote access is provided on an as-needed basis; email messages and documents are not to be forwarded to personal email accounts nor transferred to personally owned computers or devices by other means (including but not limited to external USB devices).

All remote access is centrally managed by the designated IT Administrator and utilizes encryption and strong authentication measures.

It is the responsibility of any employee with remote access privileges to ensure that their remote access is as secure as possible. WPA or other industry standard encryption is the minimum requirement for Wi-Fi connections.

All remote access activity is subject to the Municipality's Acceptable Use of Technology Policy.

Employees that use remote access agree to never disclose their passwords to anyone, particularly to family members or friends if business work is conducted from home.

All remote access connections will include a "time-out" system, as outlined in the Unattended Computers section of this policy.

The remote access user agrees to immediately report to their Manager and the designated IT Administrator via the Help Desk any incident or suspected incidents of unauthorized access and/or disclosure of municipal resources, databases, networks, etc.

Monitoring of the Electronic Network

Municipality of Port Hope's electronic network and systems are monitored continuously to check for breaches of the security systems and/or to ensure compliance with this policy.

All traffic originating or terminating on Municipality of Port Hope's network may be recorded.

Regular monitoring of the electronic network will be completed in a manner that strikes a balance between protecting individual privacy rights and facilitating the necessary auditing and review of unacceptable and unlawful use. A routine analysis does not involve reading the content of electronic mail or files.

If due to a routine analysis or a complaint, there is reasonable suspicion of misuse of the network, special monitoring without prior notice may occur. All investigations will be undertaken in accordance with the *Charter of Rights and Freedoms, the Privacy Act and the Criminal Code.*

All staff will accommodate any request from the designated IT Administrator to provide access to and allow for inspection of any municipally owned technology asset.