Policy Number: IT-AU-02
Issued: 2018-Nov-27
Division: Information Technology

Appropriate Use of IT Resources Policy

1.0 Policy Statement

The City understands that it is important for City employees to make full use of the City's IT resources for business-related activities. The City of Mount of Mount Pearl employees shall comply with the guidelines established in this policy. The City of Mount Pearl has established a set of guidelines for the proper use of City-owned IT resources to protect the confidentiality of information, the integrity of City's records, and to protect IT resources and City assets and City business continuity. This policy conforms with the *Access to Information and Protection of Privacy Act*, and with other regulatory requirements as well as with the City's policies.

2.0 Scope

This policy applies to City of Mount Pearl employees, subcontractors, contractors and volunteers using City's IT resources. This policy covers internet usage, cellphones, and various digital storage devices, personal computers and telephones.

3.0 Purpose

To establish guidelines for City of Mount Pearl employees on the appropriate usage of City owned IT resources and to establish appropriate limits on the use of IT resources.

4.0 Definitions

- **Confidential information**:

Any non-public information disclosed to the City whether orally, in writing, by a third party, through any means of communication, by or on behalf of the disclosing party. It also included nonpublic information that the City designates as being confidential or which under the circumstances surrounding disclosure ought to be treated as confidential by any recipient.

- **IT resources:**

For the purpose of this policy, IT resources encompass internet, email service, mobiles, computers, telephones and storage locations such as shared drive and OneDrive.

- **Users:**

All City Employees, as well as everyone who have been authorized access to City's IT resources including but not limited to contractors, volunteers, students and volunteers.

5.0 General Principles

Employees, contractors and volunteers using City owned IT resources shall adhere to the following guidelines:

- City of Mount Pearl shall provide IT resources to employees, contractors and volunteers for business use only to carry out City services and obligations.
- No person shall access City-owned IT resources other than those which have been properly authorized to access by the Manager of Information Technology.
- Authorized users of City-owned IT resources have a responsibility to use them in a way that is lawful, follows City of Mount Pearl's policies, and is consistent with the purposes for which they were intended.
- The City of Mount Pearl reserves the right to establish technical standards in terms of hardware and software as deemed appropriate. All authorized users will be required to follow these standards.
- IT resources shall not be used in any way that interfere with the user's responsibilities; distract other employees from work; interfere with the performance of their duties; break rules set forth by this policy and any other policies.
- The City encourages employees not to use IT resources outside of business activities.
- The use of IT resources complies with relevant provincial laws and regulations, any illegal use of IT resources will be dealt with accordingly.
- Employees are reminded that the use of internet shall be reserved for business use only and internet activity shall be restricted within the scope of the law.

6.0 Information Management Requirements

Any work-related information created, sent or received on City-owned IT resources is a City record that must be managed according to the City's records management requirements. This applies to documents created and or received on mobile devices.

Users should avoid using instant text messaging to convey decisions, approvals, directions and other substantive business.

Employees and users are required to comply with the following parameters for choosing appropriate storage:

Directory	Used for
Laserfiche	Storing business records. Using for both working and final copies of documents.
Shared Drive	Storing business records. Used for both working and final copies of documents.
Personal Drive H:	Storing personal work-related records (e.g., personal plans, reports).
C: Drive	Only as back up storage when network is down. Once normal system settings have been restored, work done on C: drive should be transferred to the appropriate folder on the shared directory.

One Drive	Storing personal work-related records and also for sharing information and documents to third parties.

7.0 Compliance

Users should be aware that any record retained on City owned IT resources and equipment is in custody and under control of the City and therefore, may potentially be subjected to a request for information under the Access to Information and Protection of Privacy (ATTIP).

Information stored on City's equipment that is subjected to ATTIP requests may not be deleted after the request has been received until the response has been provided and all applicable review periods have expired.

8.0 Loss and Theft

City employees and users will take all reasonable measures to protect City-owned IT equipment assigned to them against being misplaced, lost or stolen. In case of loss or theft of a device, users must report the incident to the Manager of Information Technology immediately as a matter of urgency.

9.0 Enforcement

Inappropriate use of the City's IT resources will be investigated on a case-by-case basis. Any employee found to have violated the policy may be subject to disciplinary action that may lead to suspension from the use of IT resources, and up to and including termination of employment.

10.0 Approvals

Steve Kent, Chief Administrative Officer

November 27, 2018

Date