THE MUNICIPALITY OF THE COUNTY OF RICHMOND
LA MUNICIPALITÉ DU COMTÉ DE RICHMOND

POLICY NAME: INTERNET USAGE & ELECTRONIC COMMUNICATION POLICY

APPROVAL DATE: MAY 26, 2014

1. Policy Statement:

The Municipality of the County of Richmond ("the Municipality") recognizes the essential role of technology in the enrichment of workplace productivity. As such, the Municipality provides employees and elected officials with access to technology and network services including Internet use and email for business purposes. This policy provides guidelines governing the appropriate use of the municipal network and systems to ensure the long-term integrity of the information technology (IT) infrastructure.

2. Applicability:

This policy applies to all authorized users of the Municipality's technology and network services, including: municipal staff (including temporary and contract employees, volunteers, students, and interns), elected officials, and other authorized organizations or individuals.

The roles and responsibilities of IT staff, as outlined in this policy, do not extend to the maintenance of non-municipally owned technology.

3. Definitions:

3.1. System refers to a communication device designed to accept data, perform prescribed mathematical and logical operations at high speed, and display the results of these operations. Such devices include computers (e.g., desktop, laptop), tablets, mobile devices (e.g., cell phones, smart phones), and landline telephones.

3.2. Network refers to a collection of systems interconnected by communication channels that allow sharing of resources and information. Includes connectivity to the Internet where applicable.

3.3. Server refers to a hardware system that supplies data or resources to other systems on a network.

3.4. Peripheral is a device attached to a host system, but not part of it, and is more or less dependent on the host. It expands the host's capabilities but does not form part of

the system's core structure. Common peripherals include, but are not limited to: printers, fax machines, digital cameras, data storage devices (e.g., flash drives), projectors, keyboards, speakers, and monitors.

3.5. Document refers to any kind of file that can be read on a system as if it were a printed page. These include, but are not limited to: web pages, emails and files meant to be accessed by documentation or data management software (e.g., Microsoft Office applications), or an electronic publishing tool (e.g., Adobe Acrobat).

4. Guiding Principles

The following principles will guide the IT practices of the Municipality:

4.1. Efficiency – to provide seamless IT infrastructure, tools and services in support of the administrative process of the Municipality.

4.2. Professionalism – to require that network use and information sharing is used ethically and primarily for business-related purposes.

4.3. Integrity: to ensure that municipal staff and Council conduct themselves honestly and appropriately in all forms of communication, respecting the laws governing copyright infringement, intellectual property, software licensing, property rights and privacy.

4.4. Accountability – to require that all municipal staff and Council are responsible for understanding and following the relevant policies and procedures affecting system, network, and Internet usage.

4.5. Security – to continually monitor, evaluate and improve the technology and practices employed to secure the Municipality's networks, servers and systems.

4.6. Legislative – to adhere to applicable provincial, federal and municipal laws, regulations and policies.

5. Roles and Responsibilities

5.1. **Council** (or its designated committee) will:

a. ensure that the Municipality has in place a comprehensive Internet Usage & Electronic Communication Policy.

5.2 The **Chief Administrative Officer** will:

a. administer and implement the Internet Usage & Electronic Communication Policy of the Municipality, and;
b. identify necessary revisions to the Internet Usage & Electronic Communication Policy in collaboration with the IT Coordinator;
c. authourize any purchasing and installing of all software associated with the Municipality's servers, systems, peripherals, and any other devices connected to the network.

5.3 The **IT Coordinator** will:

a. make recommendations to the CAO for any purchasing and installing of all software associated with the Municipality's servers, systems, peripherals, and any other devices connected to the network;
b. remain knowledgeable of new concepts to assess and promote the use of technology and ensure continuous IT training opportunities are available for all municipal staff and councillors.
c. provide assistance and support to municipal staff and councillors to maximize their use of systems and the municipal network, and;
d. report any observed and/or suspected incidents of non-compliance to the immediate supervisor of the individual suspected of being in violation said policy

5.4 **Directors** will:

5.4.1 ensure that staff are familiar with the Internet Usage & Electronic Communication Policy as located in the policy manual;
5.4.2 address any inappropriate activity conducted by staff, and;
5.4.3 identify necessary revisions to the Internet Usage & Electronic Communication Policy in collaboration with the IT Coordinator and CAO.

7. TERMS OF USE

7.1. **Acceptable Usage**

- In recognition of the need that most employees and elected officials have to take care of occasional personal matters during work hours, reasonable personal use of systems is allowed, provided that it does not interfere with Municipal business.
- In accordance with Section 100D of the *Motor Vehicles Act*, the use of portable systems (e.g., mobile phones and tablets) is prohibited while operating Municipal vehicles or private vehicles in the conduct of Municipal business.

7.2. **Appropriate content**

- The following are categories of websites are prohibited from access and should not be visited by municipal users under any circumstances:
  - file sharing and piracy sites;
  - sites that promote, foster, or perpetuate discrimination on the basis of race, creed, colour, age, religion, gender, marital status, physical or mental disability, or sexual orientation;
  - sexual content or links to sexual content, and;
  - sites that promote illegal activities as defined by the *Criminal Code of Canada* and provincial regulations.

- Users who accidentally discover that they can connect to these sites or other potentially offensive material, must immediately disconnect from these sites and alert the IT Coordinator and/or the CAO of the occurrence.

7.3. **Safety & Security**

- Municipal systems have been configured to provide protection against viruses and malicious software. Users are prohibited from changing or disabling these security settings as they are intended to protect the privacy and security of all users connected to the network.
- Users are prohibited from downloading and installing non-standard software on municipal systems and connecting peripheral devices to systems on the network without approval from IT staff.

7.4. **Personal Accountability**

- The sharing of user names and passwords obtained for access to the network and Internet resources is strictly prohibited. Any staff or elected official who obtains a user name and password for a municipal system must keep that password confidential.
- Users of municipal Internet facilities shall identify themselves honestly, accurately, and completely when participating in electronic communication (e.g., email) and other interactive Internet-based activities (e.g., social media).
- The activity records for individual system and network usage – including but not limited to call history, emails, text messages, and Internet access – is information that may have to be released to the public, if requested, under Part XX of the *Municipal Government Act* regarding Freedom of Information and Protection of Privacy.