SUBJECT: Computer and Technology Acceptable Use Policy (FCS09016) (City Wide)

RECOMMENDATION:

a) That the Computer and Technology Acceptable Use Policy, attached as Appendix “A” to report FCS09016, be approved; and

b) That the Computer Acceptable Use Policy (approved by Council January 8, 2003) be repealed.

Antonio D. Tollis
Acting General Manager
Finance and Corporate Services

EXECUTIVE SUMMARY:

The Computer Acceptable Use Policy was approved by Council on January 8, 2003. Since then, many things have changed both in the City’s technology landscape and in technology usage patterns in the community.

The policy has been updated and strengthened to clarify the City’s expectations regarding the use of technology provided by the City to its’ employees and elected officials. Also, the policy has been renamed as the “Computer and Technology Acceptable Use Policy” to reflect its’ applicability to a wider range of technology.
BACKGROUND:

A review of the Computer Acceptable Use Policy (approved by Council on January 8, 2003), revealed the need for an update to address changes in technology, legislation and usage patterns.

Since the existing policy was drafted, the technologies used by the City have changed significantly. City staff and elected officials now use Blackberries, tablet computers, wireless communications and USB memory devices. Internet services such as FaceBook, MySpace, YouTube and others did not exist when the current policy was developed. New legislation being introduced in the fields of privacy and copyright has also changed the environment.

A clear and comprehensive policy addressing the use of technology within the City of Hamilton is important for the following reasons:

- To set clear expectations for authorized users to ensure that there are no misunderstandings around the use of this corporate service; and so that authorized users are aware of the impact of Human Rights and ethics issues in the virtual workplace.
- To protect the City’s computer and network services from both inadvertent and malicious damage caused by the introduction of viruses, hacking or unauthorized uses.
- To avoid or address privacy issues.
- To avoid liability for issues such as inappropriate or illegal email content or Internet use.
- To monitor, audit and control Internet use and server storage to prohibit unacceptable uses and to control costs.

Software and hardware tools are required to support the policy. These will include tools to improve the security of City computers, to improve the reporting and filtering of Internet activity and to improve the logging of events required for the tracking and investigation of incidents of inappropriate use. Approval for the acquisition of these tools will be included in the 2010 capital budget submission.

As part of the implementation of the Computer and Technology Acceptable Use Policy, a comprehensive communications plan will be developed to ensure that all authorized users are aware of and understand the policy.

The policy was reviewed by a workgroup involving Human Resources, Legal Services and Information Services. Input was also obtained from staff in several City divisions and the draft policy was also reviewed by members of the Information Services Working Committee.
ANALYSIS/RATIONALE:

As a result of the review by the workgroup and consultation with other City departments
And because of the rapid changes in the information technology field;
And because of the liability risk to the City;

it is recommended that there is no alternative to establishing a comprehensive and effective Computer and Technology Acceptable Use Policy.

ALTERNATIVES FOR CONSIDERATION:

None.

FINANCIAL/STAFFING/LEGAL IMPLICATIONS:

Legal Services has advised that the proposed policy does not contravene the following legislation which was considered in preparation of this policy:

- Municipal Freedom of Information and Protection of Privacy Act
- Human Rights Code
- Copyright Act
- Criminal Code of Canada

The software and hardware tools required to support the policy will be included in the 2009 capital budget submission.

POLICIES AFFECTING PROPOSAL:

The Computer Acceptable Use Policy, approved on January 8, 2003 will be replaced by this Computer and Technology Acceptable Use Policy.

RELEVANT CONSULTATION:

- Human Resources
- Legal Services
- Information Services
- Staff in the following divisions:
  - Economic Development and Real Estate
  - Strategic Services, Community Services
  - Customer Service
  - Family Health
By evaluating the “Triple Bottom Line”, (community, environment, economic implications) we can make choices that create value across all three bottom lines, moving us closer to our vision for a sustainable community, and Provincial interests.

Community Well-Being is enhanced. □ Yes ☑ No

Environmental Well-Being is enhanced. □ Yes ☑ No

Economic Well-Being is enhanced. □ Yes ☑ No

Does the option you are recommending create value across all three bottom lines? □ Yes ☑ No

Do the options you are recommending make Hamilton a City of choice for high performance public servants? ☑ Yes □ No

The creation of a respectful, desirable and supportive workplace.
COMPUTER AND TECHNOLOGY
ACCEPTABLE USE POLICY

1. POLICY STATEMENT AND PURPOSE:

1.1 The City of Hamilton provides employees, elected officials and other organizations and individuals with access to Computer and Network Services, including Internet use and email, to be used for legitimate business purposes in serving the interests of the City. These technologies are valuable tools that enable Authorized Users to effectively carry out the City’s business. As such, they must be used in a responsible and appropriate manner.

1.2 This Policy outlines the City’s expectations regarding the use of these Computer and Network Services and sets clear parameters for Authorized Users to ensure clarity surrounding the use of this corporate resource. The use of this corporate resource is not a right but a privilege and is subject to the terms of this Policy. Prior to the use of the City’s Computer and Network Services, all Authorized Users are required to read this Policy and electronically acknowledge their agreement to comply with it.

1.3 Authorized Users are expected to practice good judgment and to demonstrate a sense of responsibility and consideration of others when using the City’s Computer and Network Services. All work undertaken shall be performed in an ethical and lawful manner, demonstrating integrity and professionalism by all users.

2. SCOPE:

2.1 This Policy applies to all Authorized Users of the City’s Computer and Network Services.

3. DEFINITIONS:

3.1 “Authorized Users” includes all City employees (including full-time, temporary, part-time, and contract employees, volunteers, students and interns), elected officials and other authorized organizations or individuals.

3.2 “Computer and Network Services” means all:

(i) computer software, data processing, hardware and equipment owned and/or leased by the City, including desktop, laptop, tablet, notebook, server or handheld computers (such as BlackBerry or other PDA), telephones, including IP, cellular or traditional phones, scanners, printers and fax machines and peripheral devices and removable media associated with the computer (such as USB memory sticks, CDs, etc); and
(ii) transmission methods and services employed by the City’s computer hardware and equipment, including wired, wireless and cellular networks, whether accessed from within the City’s premises or elsewhere.

3.3 “Non-public Information” means information that is exempt or is potentially exempt from disclosure under the Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56 or the Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Schedule A, or that is otherwise deemed confidential.

4. ACCESS:

4.1 Authorized Users have access to the City’s Computer and Network Services.

4.2 Access to these Computer and Network Services enables Authorized Users to conduct City business, to perform assigned duties, to research and obtain information relevant to City business and to provide information to residents, businesses and business prospects of the City of Hamilton.

5. CITY PROPERTY:

5.1 All files and electronic communications, including email, Internet and web content systems, created on, generated by or transmitted through the City’s Computer and Network Services are deemed to be the property of the City of Hamilton.

6. MONITORING:

6.1 All Authorized Users should be aware that the City’s Computers and Network Services create activity records, including but not limited to, every Internet site visited and every message sent.

6.2 While the City of Hamilton respects the privacy of Authorized Users, it still reserves the right to monitor use of its Computer and Network Services, including any email labeled “private”. Authorized Users should be aware that they have no right of ownership or expectation of privacy with regards to their use of the City’s Computer and Network Services and use will be monitored for appropriateness and to assist in protecting and maintaining security. The City reserves the right to take action, including accessing any files, information and equipment, without notice.
7. USAGE:

7.1 The City’s Computer and Network Services, including Internet and email systems, are corporate resources. The primary use of the Computer and Network Services is for business purposes.

7.2 Limited, occasional or incidental use of the Computer and Network Services for personal activities is acceptable, provided the privilege is not abused. Personal uses involving substantial expenditures of time, uses for profit or uses that would otherwise violate any City policy are not permitted. Any inappropriate, excessive or abusive usage may result in an Authorized User’s access privileges being limited or revoked, and City employees may also be subject to disciplinary measures up to and including dismissal.

7.3 The City reserves the right to filter and quarantine both inbound and outbound electronic content, including but not limited to email and web content, in order to ensure the availability, reliability and security of the Computer and Network Services.

7.4 The City retains the right to report any illegal violations to the appropriate authorities.

7.5 The City’s existing corporate and human resources policies, including “Code of Conduct”, “Harassment and Discrimination Prevention”, “Personal Harassment Prevention”, and “Race Relations”, and the City’s “Code of Conduct for Members of Council” also apply to conduct while using the City’s Computer and Network Services.

7.6 Authorized Users are expected to adhere to the following:

7.6.1 Authorized Users shall not distribute outside of the City’s internal network any Non-public Information, unless such distribution has been properly authorized and, where necessary, properly protected (e.g., encrypted, password-protected).

7.6.2 Authorized Users shall conduct email messaging in the same manner as they would other business correspondence, being mindful of the fact that email transmissions over the Internet are not secure and may be intercepted, and that email is subject to the provisions of the Municipal Freedom of Information and Protection of Privacy Act. Authorized Users are responsible for all email sent from their individual user name and should take appropriate precautions to ensure that their password is changed regularly and is not shared with anyone, except within the terms of this Policy.
7.6.3 Authorized Users shall not, in any way, attempt to access confidential information to which they have not been previously granted access.

7.7 Social networking sites such as Facebook and MySpace are recognized as useful tools for communicating and collaborating with the public in appropriate circumstances. Authorized Users should use these sites primarily for City business purposes as approved by the Authorized User’s management.

7.8 Authorized Users must comply with copyright and licensing restrictions on any information which has been downloaded. Material which is viewed, copied, scanned, downloaded or saved from the Internet should be primarily related to City business.

7.9 Authorized Users must abide by vendor license agreements. Use of applications and/or data is subject to the vendor’s license agreement and may not be reproduced in any form without permission from the vendor.

7.10 Authorized Users must protect proprietary information, including computer software and documentation belonging to the City, its customers, or vendors, in accordance with contractual restrictions and City policies.

7.11 Any acquisition of goods or services must be in accordance with the City’s Purchasing Policy.

7.12 Authorized Users may not offer goods or services over the Internet or on the City’s network for personal use, nor may they send “for sale or wanted to buy” messages on the Internet or by email. This does not prohibit any approved personal “Buy and Sell” page on eNet, the City’s Intranet site.

7.13 Authorized Users are obliged to follow security and data practices provided by Information Services to protect City information.

7.14 Authorized users who are permitted to access the City’s Computer and Network Services remotely (e.g., from home) using a VPN connection and their personal computer must ensure that their personal computer is safe to use, including the use of a personal firewall and an up-to-date anti-virus scanner.

7.15 Authorized Users should be familiar with the Information Services guidelines posted on eNet, the City’s Intranet site.

7.16 Authorized Users are required to report any damage to or loss of City property covered by this Policy to Information Services immediately. The City is not responsible for any misuse of the Computer and Network Services. Persons found to be misusing the City’s resources will be responsible for any costs or damages sustained by the City or a third
party, and will be obligated to indemnify the City for any claims against the City.

7.17 Acceptable and appropriate usage includes, but is not limited to the following list:

7.17.1 Participating in professional, work-related research.

7.17.2 Distributing work-related correspondence, minutes, agendas and reports.

7.17.3 Responding to public inquiries.

7.17.4 Accessing work-related distance learning opportunities.

7.17.5 Creating work-related information resources.

7.17.6 Participating in work-related mailing lists or forums.

7.17.7 Communicating with staff, elected officials, and appropriate outside bodies such as other levels of government, businesses, City partners, citizen groups and residents.

7.18 Unacceptable and inappropriate usage includes, but is not limited to, the following list. The only exception is in the performance of work-related matters as approved by a member of the City’s Senior Management Team:

7.18.1 Accessing sites or transmitting material which violates any Canadian federal or provincial law or City by-law or directive, such as defamatory, discriminatory or obscene material or sites which, in the opinion of management, are inappropriate.

7.18.2 Accessing, displaying or storing email messages, graphics or images on the City’s Computer and Network Services that are obscene, harassing or fraudulent or that are offensive and conducive to a poisoned work environment. (Inadvertently accessing an inappropriate site or receiving an email with an unacceptable attachment will not be considered a violation of this Policy. Printing, scanning, saving or forwarding inappropriate material, except as properly authorized, shall be considered a violation of this Policy.)

7.18.3 Distributing to members of the public, Non-public Information such as draft reports, confidential information or information without proper authorization and, where necessary, proper protection.
7.18.4  Downloading files or introducing removable media to City computers without virus scanning with an approved and up-to-date virus scanner. Authorized Users are responsible for ensuring that their virus scanning software is up-to-date.

7.18.5  Installing and using software banned for security reasons, including but not limited to: Kazaa, Morpheus, LimeWire, Donkey 2000, Bear Share, Gnutella, Nutella, iMesh, Blubster, and Instant Messaging applications such as AIM (AOL Instant Messenger), ICQ, NET, MSN or Windows Messenger, Yahoo Messenger Services.

7.18.6  Downloading or storing on the City’s network servers any non-work-related photo, music or video files.

7.18.7  Sending chain letters, junk mail or broadcast transmissions (i.e., sending a single message to a large number of individual email addresses) unless approved by the Authorized User’s management.

7.18.8  Using the Internet to access personal email accounts, including those provided by your personal Internet Service Provider (e.g. Rogers, Cogeco, Sympatico, etc) and web-based email systems (e.g. Hotmail, Yahoo, gMail, etc.) from within the City’s network. Note that this restriction refers to logging on and opening mailboxes in these email systems. Authorized Users may use the City’s email system to correspond with users of any type of email system.

7.18.9  Participating in Internet chat groups or mailing lists that are not work-related.

7.18.10  Storing games, game-related data or personal web site material on any City network server.

7.18.11  Sending anonymous messages or accessing the Internet under another person’s network identification.

7.18.12  Allowing others who are not Authorized Users to access and utilize the City’s Computer and Network Services.

7.18.13  Sharing City accounts or passwords with any other person, except as authorized by a member of the City’s Senior Management Team.

7.18.14  Making unauthorized copies of copyrighted software. It is the responsibility of individual departments to ensure they obtain the appropriate software licensing and the responsibility of
Authorized Users to obtain appropriate licensing for home computers.

7.18.15 Changing the configuration of the City’s Computer and Network Services without authorization from Information Services.

7.18.16 Circumventing City computer security measures, attempting to gain access to a City system for which proper authorization has not been given, probing the security at any computer site or accessing sites or tools dedicated to computer/network hacking.

7.18.17 Connecting unauthorized devices (including personal or vendor laptops) to the City’s network without obtaining prior approval from Information Services.

7.18.18 Leaving City computers logged on or unlocked when leaving the workplace for any extended period.

8. AUDITING:

8.1 Where there are reasonable grounds to suspect that an Authorized User has abused or contravened this Policy, an audit of the Authorized User’s usage may be undertaken, with or without notice to the Authorized User.

8.2 Usage audits of City employees may be requested by a member of the City’s Senior Management Team. The audit will be conducted by Information Services in concert with the requesting department.

8.3 Usage audits of elected officials or their staff may be requested by Council. Records required for the audit will be collected by Information Services and provided to the auditing body authorized by Council.

8.4 Usage audits of any Authorized User may be requested by law enforcement officials. In the event of such a request, records required for the audit will be collected by Information Services and provided to law enforcement as required by law or otherwise authorized by legislation.

9. COMPLIANCE:

9.1 Failure to comply with this Policy may result in the Authorized User’s access privileges being limited or revoked and City employees may also be subject to disciplinary measures up to and including dismissal.

10. ADMINISTRATION:

10.1 This Policy is administered by the Corporate Services Department, Information Services Division.
RELEVANT LEGISLATION:

- *Copyright Act*, R.S., 1985, c. C-42
- Purchasing Policy for the City of Hamilton

COUNCIL REFERENCE:

Approved by Council of the City of Hamilton on ____________, 2009, in report no. FCS09016.

CONTACT:

For more information or procedures, contact Information Services, Corporate Services Department.