City of Seattle
Policy and Procedure

Subject:		Number:
City-owned Technology Resource Acceptable Use Policy		**N/A**
		Effective: June 24, 2010
Authors: City of Seattle Office of Information Security, et al.		**Supersedes:** ISSP POL17: Acceptable Use of City Digital Equipment, Internet Access, E-Mail and Other Applications; all versions of this policy prior to the date above.
Approved: Bill Schrier, Chief Technology Officer	**Department:** Citywide	**Page(s): 5**

1.0 PURPOSE:

This policy defines the appropriate use of technology resources that are owned by the City of Seattle and provided for employee use. Departments are permitted to issue their own policies that augment or adopt this policy through reference, but not to supersede or contradict it.

2.0 APPLICABILITY:

This policy applies to anyone who uses City Technology Resources, including employees, temporary employees, contractors, vendors and all others.

3.0 DEFINITIONS:

3.01 Internet: the Internet is a worldwide "network of networks," including bulletin boards, World Wide Web (WWW), data servers, applications, messaging services, and other functions and features, which accessed via a computer, a BlackBerry, or other client devices.

3.02 Digital Equipment: Includes but is not limited to computers, laptops, telephones, cellular telephones, Personal Digital Assistants (PDAs), and combination devices such as Blackberries. Any technology provided by the City for communications, computing, printing, etc. is covered by this definition.

3.03 Data Files: Information contained in files such as e-mail messages, database tables, telephone records, extracts from databases or output from applications.

3.04 Messaging: Any technology used to facilitate digital communication, including but not limited to Instant Messaging (IM), electronic mail (e-mail, both City-provided and through external services for personal use), peer-to-peer networking (P2P), mobile, fixed, and software-based voice over Internet protocol (VoIP) telephones.

3.05 City-owned Technology Resources: Technology resources paid for by city funds, including, but not limited to: Internet/Intranet/Extranet-related systems, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, and systems that enable web browsing, and file transfer.

3.06 Social Networking: Any Internet site that is focused on creating "networks" of individuals such as MySpace, FaceBook, LinkedIn, etc.

3.07 Hacking/Hacking Tools: Behavior and tools designed to circumvent security measures, or to otherwise effect unauthorized changes to computer hardware or software.

3.08 Peer-To-Peer Networking: Protocol or service for networking devices without a centrally managed server.

3.09 Communication protocol: An agreed-upon method of communication used within networks.

3.10 Malware: A general term for potentially hostile software; encompasses viruses, Trojans, spyware, etc.

4.0 POLICY:

4.01 City Resources are for City Business: City-owned technology resources shall serve the business needs of the City of Seattle.

4.02 Confidentiality: City-held information on the constituents of the City of Seattle may not be disclosed without a clear business need, or public disclosure request.

4.03 Limited Personal Use: City owned technology resources may be used for personal purposes on a limited basis, providing the following requirements are met:

- No marginal cost to the City
- No interference with work responsibilities
- No disruption to the workplace.

4.04 Limited use of external e-mail services: The limited use of an external e-mail service is allowed, providing that the service applies anti-malware controls in a manner equivalent to that provided by the City.

4.05 Music: City computers must not be used to store music/audio files for personal use.

4.06 Specific Prohibitions and Limitations: City policies regarding acceptable behavior and communication will apply to use of the Internet and messaging. Specifically prohibited use includes but is not limited to:

- Conducting a private business;
- Political campaigning;
- Accessing sites which promote exclusivity, hatred, or positions which are contrary to the City's policy of embracing cultural diversity;
- Accessing inappropriate sites including adult content, online gambling, and dating services;
- Accessing sites that promote illegal activity, copyright violation, or activity that violates the City's ethical standards.
- Using the internet to obtain or disseminate language or material which would normally be prohibited in the workplace;
- Using encryption technology that has not been approved for use by the City;
- The use of personally owned technology for conducting City business, where official City records are created but not maintained by the City;
- Making unauthorized general message distributions to all users (everyone);
- Installing any software that has not been approved by the City;
- Sharing or storing unlicensed software or audio/video files;
- Using security exploit tools (hacking tools) to attempt to elevate user privileges or obtain unauthorized resources;
- Broadcasting e-mail to large numbers of constituents unless the list members are hidden through the use of the BCC field.
- Using a City e-mail address when posting to public forums e.g. blogs, social media sites, wikis and discussion lists for personal use;
- Accessing sites that distribute computer security exploits ("hacking" sites);
- Excessive use of online shopping,
- Excessive use of social networking sites for personal use;
- Excessive use of streaming media for entertainment during work hours;
- The use or installation of unauthorized Instant Messaging, e.g. AIM, Yahoo Instant Messenger, Meebo, IRC, etc.; links and attachments are prohibited using the authorized IM client;
- Using unauthorized Peer to Peer Networking, e.g. E-Mule, Kazaa, Limewire, Warez, etc;
- The Use of "Soft" VOIP phones, e.g. Skype, Vonage, etc.

NOTES:

1. If any of the above prohibited uses is required for a legitimate business reason, it is management's responsibility to follow the exception process as referenced in Section 7.

4.07 Use Standard Resources Only: Digital equipment and all applications must be authorized and installed by appropriate personnel. Only software, hardware, and communication protocols that meet the City's defined standards will be installed unless an exception has been documented in writing.

4.08 Additional Cost to the City: Resources that incur a cost to the City, whether accessed via the Internet, mobile/PDA, email or other applications, must not be accessed or downloaded without prior approval. It is the supervisor's responsibility to assure the business need, applicability, and safety of any new resource.

4.09 No Expectation of Privacy: Nothing in this policy confers an individual right or be construed to provide an expectation of privacy. Employees must not expect privacy in the use of City communications and digital equipment.

4.10 Conflicts: If any component of this policy conflicts with any applicable collective bargaining agreement, the collective bargaining agreement shall control. The remaining non-conflicting features of this policy shall remain in effect.

5.0 RESPONSIBILITIES:

5.01 Employee Responsibilities

- Monitor personal use of the internet, messaging, and other applications, to ensure that the City is being appropriately served.
- Adhere to City standards as discussed in the policy language above.
- Read and adhere to relevant policies.
- Obtain authorization from their supervisor before incurring charges; for example, downloading data or accessing a paid service.
- Request Service Desk (6-1212) to download and install software unless express consent has been granted for employees to download and install software.

5.02 Management Responsibilities

- Support enterprise-grade technology to enforce this policy, to ensure that the primary purpose of that use is to meet City business needs, and that relevant City standards are met.
- Review and make decisions regarding the approval of all non-work related broadcast announcements. Acceptable uses for non-work related broadcast announcements would include arrival or departure of a department employee or a departmental charitable campaign event.

6.0 POLICY ENFORCEMENT:

In order to safeguard City resources, violators of this policy may be denied access to City computing and network resources and may be subject to other disciplinary action within and outside the City. Violations of this policy will be handled in accordance with the City's established disciplinary procedures. The City may temporarily suspend, block or restrict access to computing resources and accounts, independent of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, confidentiality, or availability of City computing and network resources, or to protect the City from liability.

6.01 If violations of this policy are discovered, the City will take appropriate actions to resolve the issue and violators may be subject to disciplinary measures.

6.02 If violations of this policy are discovered that are illegal activities, the City may notify appropriate authorities.

6.03 The City reserves the right to pursue appropriate legal actions to recover any financial losses suffered as a result of violations of this policy.

7.0 EXCEPTION PROCESS

Exceptions to this policy will be requested in writing to management, and the request will be escalated to the Office of Information Security, Human Resources, or the Office of the Chief Technology Officer. Exceptions will be documented in writing and retained according to existing retention schedules. Exceptions may be granted on a limited-time basis.

8.0 REFERENCES:

- Seattle Municipal Code Section 4.16, *Code of Ethics.*
- Seattle Municipal Code Section 2.04.300, *Political Activities*
- City Resolution 29669, *Policy on Workplace Harassment.*
- Information Systems Security Policy Handbook, March 2007
- City Guidelines on Employee Use of City Equipment and Facilities, revised 8/2/99
- DPAC Standards 5.1 *Email Usage*, adopted October 11, 1994.
- DPAC Standards 5.2 *Internet Acceptable Use*, adopted May 9, 1995.
- DoIT Workplace Expectations
- Applicable Labor Agreements

Revision History

Version	Description	Written By	Date	Authorized By
1.0.0	Policy enacted	Mike Hamilton	11-3-2008	Bill Schrier
1.1.0	Corrected spelling error, added prohibition on City address on social networking sites, and revision history block	Mike Hamilton	6-24-2010	City IT Governance