# City of Seattle
# Policy and Procedure

| Subject: | | Number: |
|---|---|---|
| **City-owned Technology Resource Acceptable Use Policy** | | **N/A** |
| | | **Effective:** **TBD** |
| **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:** **Michael Mattmiller, Chief Technology Officer** | **Department:** **Citywide** | **Page(s): 7** |

## 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, social media, and other functions and features, which are accessed via a computer, a mobile device, or other client devices.

3.02 Digital Equipment (Device): Includes but is not limited to computers, laptops, telephones, cellular telephones, smart phones, and other devices such as tablets. 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, electronic documents, 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), SMS (texting), audio and video conferencing, 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 and other digital equipment, software, operating systems, storage media, network accounts providing electronic mail and other messaging, and systems that enable web browsing, and file transfer.

> 3.05.1 Non-City-owned Technology Resources: Technology resources NOT paid for by City funds, including, but not limited to: Internet/Intranet/Extranet-related systems, computer and other digital equipment (including but not limited to tablets, laptops, smartphones), software, operating systems, storage media (including but not limited to USB or "flash" drives, external hard drives, camera memory, cloud storage media), accounts providing personal electronic mail and other messaging or social media, and systems that enable web browsing, and file sharing.

3.06 Social Media: Any Internet site such as blogs, Facebook, Twitter, LinkedIn, YouTube, etc. that is focused on creating "networks" of individuals.

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.

3.11 City Records or Public Records: Any writing containing information relating to the conduct of City government or the performance of any City governmental or proprietary function prepared, owned, used, or retained by the City, including any City employee, regardless of physical form or characteristics.

3.12 Washington Public Records Act: Chapter 42.56. Revised Code of Washington (RCW)

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

4.03 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.

4.04 Limited Personal Use: City owned technology resources may be used for personal purposes on a limited basis, providing this use results in:

- 4.04.1 No marginal cost to the City
- 4.04.2 No interference with work responsibilities
- 4.04.3 No disruption to the workplace
- 4.04.4 No storage of unlicensed, copyrighted materials on any City-owned technology resources.
- 4.04.5 No device-to-device connection of Non-City-owned Technology Resources to City-owned Technology Resources. For example, charging of personal smartphones via City computer USB port is prohibited.
- 4.04.6 No illegal activities.
- 4.04.7 No commercial or solicitation activities.

4.05 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, and such use is incidental and does not interfere with your workload, as determined by your supervisor. Attachments and embedded links should not be clicked or downloaded.

4.06 Media Files: City computers, devices, and other storage locations must not be used to download or store music/audio/movies/eBooks/games files for personal use.

4.07 Sharing of City Data Files: City Data Files may be shared as needed to support City functions and in accordance with the Information Systems Security Policy, In particular:

- POL10 Electronic Data and Records Management
- GUI10A Classification of Data

4.07.01 Data files classified as PUBLIC may be shared without restriction except where copyright is applicable.

4.07.02 Data files classified as SENSITIVE should be shared only when the City has a documented business need, or as required under the Washington Public Records Act pursuant to specific public disclosure requests. To the extent that non-disclosure is allowed under law. Restricted data files should be shared only when

the integrity and obligations of the City's business operations and compliance requirements are ensured.

4.07.03 Data files classified as CONFIDENTIAL should not be shared except as required to conduct City business. It is specifically protected in all or in part from disclosure under the State of Washington Public Disclosure Laws.

4.07.04 Data files classified as CONFIDENTIAL REQUIRING SPECIAL HANDLING is specifically protected from disclosure by law and subject to strict handling requirements dictated by statues, regulations, or legal agreements.

4.08 Downloading to and Storage of City Records on Non-City-owned Technology Resources:

4.08.01 City or Public Records should not be downloaded to, nor stored on Non-City-owned Technology Resources unless by exception granted by the Chief Technology Officer.

4.08.02 City or Public Records stored on Non-City-owned Technology Resources are subject to the same regulations concerning disclosure, discovery and records retention as City records stored on City-owned Technology Resources. The storage of any City or Public Record on any device may subject the entire device to a search for records under the Washington Public Records Act, or under court rules related to discovery in litigation.

4.09 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:

4.09.1 Conducting a private business;
4.09.2 Political campaigning;
4.09.3 Accessing sites which promote exclusivity, hatred, or positions which are contrary to the City's policy of embracing cultural diversity;
4.09.4 Accessing inappropriate sites including adult content, online gambling, online gaming, and dating services;
4.09.5 Accessing sites that promote illegal activity, copyright violation, or activity that violates the City's ethical standards.
4.09.6 Using the internet to obtain or disseminate language or material which would normally be prohibited in the workplace;
4.09.7 Using encryption technology that has not been approved for use by the City;
4.09.8 Making unauthorized general message distributions to all users (everyone);
4.09.9 Installing any software that has not been approved by the City;

4.09.10 Sharing or storing unlicensed software or audio/video files;

4.09.11 Using security exploit tools (hacking tools) to attempt to elevate user privileges or obtain unauthorized resources;

4.09.12 Broadcasting e-mail to large numbers of external constituents unless the list members are hidden through the use of the BCC field.

4.09.13 Using a City e-mail address when posting to public forums e.g. blogs, social media sites, wikis and discussion lists for personal use;

4.09.14 Accessing sites that distribute computer security exploits ("hacking" sites);

4.09.15 Use of online shopping and/or interferes with your workload, as determined by your supervisor.

4.09.16 Excessive use of social media sites for personal use that is more than incidental, and/or interferes with your workload, as determined by your supervisor.

Use of streaming media for other than City of Seattle business purposes during work hours;

4.09.18 Using unauthorized Peer-to-Peer Networking

4.09.19 Using a City e-mail address as a means of notification for personal use, e.g. shopping, dating or social media sites.

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.

4.10 Use Standard Resources Only: All Digital equipment and 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 on, or connected to, City-owned Technology Resources unless an exception has been granted and documented in writing.

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

4.12 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

5.01.1 Monitor personal use of the internet, messaging, and other applications, in accordance with Sections 4.01-4.12 above.

5.01.2 Monitor the sharing of City data files in accordance with Section 4.07, above

5.01.3 Adhere to City standards as discussed in the policy language above.

5.01.4 Read and adhere to relevant policies.

5.01.5 Obtain authorization from their supervisor before incurring charges; for example, downloading data or accessing a paid service.

5.01.6 Request the applicable Service Desk to download and install software to City-owned Technology Resources unless express consent has been granted for employees to download and install software.

5.02 Management Responsibilities

5.02.1 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.

5.02.2 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 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, CTO |
| 1.1.0 | Corrected spelling error,<br>added prohibition on using City address on social networking sites, and revision history block | Mike Hamilton | 6-24-2010 | City IT Governance |
| 1.2.0 | Updated with language added to address data file sharing. | Bruce Blood & Bryant Bradbury | 10-29-2015 | City IT Governance |