Attachment E

17004

King County

Addendum B

Office of Information
Resource Management

Information Technology Governance Policies, Standards and Guidelines

Title	Document Code No.
Acceptable Use of Information Technology Assets Guidelines	
Chief Information Officer Approval / Date	Effective Date.
Revision Date: 9-29-07	

1.0 PURPOSE:

These guidelines advise users of King County Information Assets on acceptable and prohibited uses. King County provides its users with Information Technology Assets and resources, including workstations, Internet access and electronic communications services for the performance and fulfillment of job responsibilities. Prudent and responsible use begins with common sense and includes respect for the public's trust, the larger networked computing community and the access privileges that have been granted. The use of such resources imposes certain responsibilities and obligations on users and is subject to King County policies and applicable local, state and federal laws. Prohibited use of computing and network resources can lead to consequences affecting the individual user, many other users, and cause service disruptions.

These guidelines, while not exhaustive, are intended to provide illustrations and guidelines for best practices of acceptable conduct by users of King County Information Technology Assets.

2.0 REFERENCES:

2.1 Enterprise Information Security Policy

2.2 Acceptable Use of Information Technology Assets Policy

2.3 King County Information Privacy Policy

2.4 Password Management Policy

2.5 Employee code of Ethics KCC 3.04

2.6 King County Board of Ethics Advisory Opinion 96-08-1146

3.0 DEFINITIONS:

3.1 **Authorization:** The right or permission to use a computer resource.

3.2 **Authorized User:** A user with the right or permission to use a computer resource.

3.3 **Computing Resources:** Any computer based system available to a King County employee. This can be a computer, database, network device, server, printer etc.

3.4 **Information Asset:** A definable piece of information, information processing equipment, or information system, that is recognized as "valuable" to the Organization that has one or more of the following characteristics:

- Not easily replaced without cost, skill, time, or other resources;
- Part of the Organization's identity, without which the Organization may be threatened.

3.5 **Minimal Personal Use**: Use that:

- Is brief in duration and frequency;
- Does not interfere with or impair the employee's ability to perform work;
- Does not interfere with or impair the conduct of official County business;
- Results in negligible or no expense to the County;
- Is not a Prohibited Use of Information Technology Assets as identified in section 5.3 in the Acceptable Use of Information Technology Assets Policy.

3.6 **Organization:** Every county office, every institution, and every department, division, board and commission.

3.7 **System**: Software, hardware and interface components that work together to perform a set of business functions.

3.8 **User:** Any individual utilizing or affecting county computer resources or information technology resources including but not limited to performing work for King County utilizing a personal computer, workstation, laptop or terminal, including but not limited to any employee, contractor, consultant, or other worker.

Note: the term "user" is used in the general sense and is not intended to imply or convey to an individual any employment status, rights, privileges, or benefits.

3.9 **Workforce Member:** Employees, volunteers, and other persons whose conduct, in the performance of work for King County, is under the direct control of King County, whether or not they are paid by King County. This includes full and part time elected or appointed officials, employees, affiliates, associates, students, volunteers, and staff from third party entities who provide service to King County.

Note: the term "workforce member" is used in the general sense and is not intended to imply or convey to an individual any employment status rights, privileges, or benefits.

4.0 GUIDELINES:

4.1 Daily Use

4.1.1 Users should not engage in any activity that would compromise the security and privacy of King County information technology resources, including but not limited to disabling virus protection, patch management or any other type of desktop management software.

4.1.2 Users should be mindful of the impact their activities have on King County shared Information Technology Assets and other users and on the need to be responsible stewards of the public's trust.

4.1.3 Users should not use King County Information Technology Assets for games, Internet radio or music, instant messaging or Internet chat applications.

4.1.4 Users should avoid using King County Information Technology Assets to watch streaming video unless necessary in the course of their duties.

4.1.5 Users should log off the network or have a password-protected screen saver in operation when they leave their PC unattended for more than five (5) minutes.

4.1.6 Users should log off the network at the end of the day since engaging a password protected screen saver is not recommended for overnight protections.

4.2 **Privacy**

4.2.1 Users should respect the privacy of others.

4.2.2 Users should use privacy screens in public areas where confidential information must be accessed.

4.2.3 Users should not forward information identified as "confidential" or "attorney client privileged" or "privileged" without permission of the author.

4.3 **Internet Use**

4.3.1 Users who inadvertently access unacceptable content on the Internet should notify organization management and provide an explanation of how, when and why the access happened.

4.3.2 Users should not post King County information to external newsgroups, bulletin boards, or other public forums without prior authorization.

4.3.3 Users should not make unauthorized statements or commitments on behalf of King County or the Organization, or post an unauthorized home page or similar web page.

4.4 **Electronic Communications**

4.4.1 Users should not access personal internet email accounts. Accessing personal mail bypasses several layers of security protection and can introduce malicious software into King County Systems.

4.4.2 Users should use extreme caution when opening email attachments, especially those received from unknown senders. These attachments may introduce malicious code into the King County network or Systems, such as viruses, logic bombs, or Trojan horses.

4.4.3 Users should clearly and accurately identify themselves on all electronic communications.

4.5 **Downloading Software**

4.5.1 Users should be aware that downloading of any software products using King County Information Technology Assets may be subject to licensing and contractual agreements.

4.5.2 Users should not download software of any kind from the Internet without the knowledge of their IT group. Such downloads can be accompanied by malicious code that could adversely affect King County's network or Systems.

4.5.3 Users should not use King County Internet access to download games or other entertainment software, or play games.

4.6 Use of Information Technology Assets

4.6.1 Users who access external networks should abide by the policies and procedures of these networks.

4.6.2 Users should exercise good judgment in their Minimal Personal Use of King County Internet access or email as defined in this policy. All Minimal Personal Use should be conducted during the employee's break times.

4.6.3 Users should use King County Information Technology Assets consistent with accepted Organization standards and in compliance with this policy.

4.6.4 Users should respect the confidentiality, availability and integrity of King County Information Technology Assets.

4.6.5 Users should not permit the use of King County owned Information Technology Assets by anyone not specifically authorized in this Policy. This includes, but is not limited to, use of laptops, PCs, and PDAs.

4.7 Remote Access

4.7.1 Users should not knowingly use remote control software on any internal or external host personal computers or Systems that organization management or Information Technology has not specifically authorized.

4.7.2 Users should not knowingly attach unauthorized modems to PCs, workstations or servers.

4.7.3 Users should not knowingly divulge dialup or dial-back modem phone numbers to anyone.

4.7.4 Users should not knowingly provide VPN access information to anyone without authorization.