SILVER LAKE WATER - SEWER DISTRICT
SNOHOMISH COUNTY, WASHINGTON
RESOLUTION NO. 648

A RESOLUTION OF THE BOARD OF COMMISSIONERS OF THE SILVER LAKE WATER-SEWER DISTRICT, SNOHOMISH COUNTY, WASHINGTON, PROVIDING FOR A POLICY TO REGULATE USE OF THE DISTRICT'S INFORMATION TECHNOLOGY SYSTEMS AND SERVICES

WHEREAS, the District has developed and will continue to develop Information Technology (IT) systems and services to facilitate improved District communications, to make information more accessible to staff for professional, learning and research purposes and to enhance and improve customer service; and

WHEREAS, the District desires to grant its staff access to its IT systems and services to facilitate District operations and to enable staff to perform their District work efficiently and effectively; and

WHEREAS, the Board of Commissioners is aware that staff access to the Internet and computing services gives rise to some risk of employee misuse of the District's IT systems and services, which could expose the District to lapses in security, breach of confidentiality, loss of data and embarrassment; and

WHEREAS the Board of Commissioners of the District has determined to adopt and implement a District IT Usage Policy providing for the general conditions of staff use of the District's IT systems and services and outlining the responsibilities of staff when using District IT systems and services.

NOW THEREFORE, BE IT RESOLVED by the Board of Commissioners of the Silver Lake Water-Sewer District, Snohomish County, Washington as follows:

1. FINDINGS The Commissioners adopt as findings the preceding recitals to this Resolution.

2. ADOPTION OF POLICY The District IT Usage Policy in the form attached hereto as Exhibit "A" is hereby adopted and approved by the Board of Commissioners. District management

3. EFFECTIVE DATE The Policy adopted hereby shall be effective as of the date of adoption of this resolution.

4. INCONSISTENT POLICIES RESCINDED All District resolutions, policies and procedures which are inconsistent with this resolution are hereby rescinded, modified and superseded to be in accordance with this resolution.

Exhibit A follows on the next page

ADOPTED by the Board of Commissioners at a regular open public meeting of the Silver Lake Water-Sewer District, Snohomish County, Washington on this 8 day of March 2010.

Rod Keppler
President and Commissioner

Bill Anderson
Secretary and Commissioner

Commissioner

I CERTIFY the above to be a true and correct copy of Resolution No. 648 adopted by the Board of Commissioners of the Silver Lake Water-Sewer District this 8 day of March 2010 as said Resolution appears in the records of the Silver Lake Water-Sewer District.

Bill Anderson
Secretary of the Silver Lake Water District

EXHIBIT "A"
Electronic Usage Policy

[SEE ATTACHED]

Electronic Usage Policy

The District respects the individual privacy of all employees; *however,* all employees should understand and be aware that they have no right to or expectation of privacy with respect to the employee's use of District provided equipment, supplies and programs, including but not limited to computer, voice mail, email, text mail, pagers, cell phones and the Internet (collectively called the District's "IT systems and services"). All information stored on and/or transmitted by District provided equipment, supplies and programs remain at all times the exclusive property of the District, and the District may monitor and review such information at any time, in the District's sole discretion. Employees should further understand that their electronic records, including but not limited to emails generated and received and Internet usage constitute "public records" which may be subject to public disclosure under the Public Records Act, Ch. 42.56 RCW. All electronic usage should therefore be made with the understanding and expectation that third parties may view such usage.

The District's IT systems and services are the exclusive property of the District and should be used for District purposes only. Unacceptable and/or inappropriate non-work related activities, including the downloading, viewing or sending of insulting, disruptive, offensive, derogatory, profane or discriminatory messages or materials are strictly prohibited. Examples of forbidden transmissions include, but are not limited to: sexually explicit messages, cartoons or jokes; sexual propositions or love letters; ethnic or racial slurs; or any other message that can be construed to be harmful to morale, harassment or disparagement of others based on their sex, race, age, national origin, religion, creed, sexual orientation, marital status, disability or any other class protected by law.

General conditions relating to employee use of the District's IT systems and services include but are not limited to the following:

- Employee use of the District's IT systems and services must at all times comply with all applicable laws and with this policy.
- Employee use of the District's IT systems and services must not interfere with others' use of such systems and services.
- Employees may not use computers for which they have not received prior authorization to use.
- Employees must not access any program or data that they have not been specifically authorized to access.
- Employees may not use District IT systems and services for purposes of engaging in non-District-related commercial activities.
- District IT systems and services may not be used to disseminate mass (unsolicited) emails.

- With the exception of District-issued cell phones, modest use of District IT systems and services for personal purposes will be permitted; provided that such use shall not occur during work time; and provided, further that such use does not interfere with the employee's or others' job performance, duties and responsibilities.

All system passwords and encryption keys must be available to the District. Employees are prohibited from the unauthorized use of passwords and encryption keys of other employees to gain access to other employee's email messages. Remember that creating a password or hitting the "delete" key does not always mean that messages or material cannot be retrieved. The District regularly backs up its email system.

All email messages sent from the District contain a header identifying the District. Because on-line communications are not secure, prior to transmitting any information that is of a confidential nature or that may include District trade secrets, authorization must first be obtained and the information must be properly encrypted. All employees are prohibited from creating or sending inappropriate messages or unprofessional communication discussing the District, its employees, customers or competitors.

The District licenses the use of computer software from a variety of outside sources. The District does not own this software or its related documentation, and it does not have the right to reproduce, use or otherwise copy that software without the permission of the software provider. Unauthorized copying or use of software or documentation on any medium is strictly prohibited. Anyone aware of any misuse of District software or related documentation must notify his or her manager. Software may only be installed on a District computer by District IT staff. No software may be installed on any District computer, including screen savers, without proper authorization. The District may, from time to time, conduct system audits to ensure compliance with this policy.

Remote access to the District network is possible via the Internet and the District's Virtual Private Network (VPN) or Remote Desktop connection. Remote access from external networks or across the Internet must be made via secure methods only. This policy applies to all remote connections as well. All remote connection attempts are logged. Non-exempt employees may not remotely log into the District's network during non-work hours, unless such employee has obtained prior authorization from his/her supervisor to do so.

Employees are expressly warned that they must respect copyright, trademark, trade secret, patent, license, policy and other proprietary rights and restrictions relating to the use, access or download of software or information. No one may download any software or information unless the following criteria have been met: (1) the information or software to be downloaded is directly related to work; (2) the District authorized the download; and (3) the District determines that the appropriate license fees have been paid.

Employees must also be careful when using electronic communication and/or software or hardware systems outside the office to maintain the confidentiality and integrity of any District information. Electronic communications should only be transmitted using equipment that has been installed with the District's spyware and security programs. Additionally, employees should at all times be mindful of their audiences in transmitting confidential communications, and should do so only when they are certain that unauthorized individuals (such as seat mates on airplanes, family members, or other people in direct proximity to the employee) will not be privy to such communications.

Web 2.0 services offer attractive and popular applications services (Blogs, wikis, office systems, social bookmarking and social networking) to mention but a few. However, making use of such services enhances and expands the risk that communications and information will be provided to unintended participants and users of such services to the potential detriment of the District. Using District computer systems and services for Web 2.0 services is prohibited without specific written authorization of the General Manager.

Employees who violate this policy shall be subject to disciplinary action, up to and including termination.