IV.6 ACCEPTABLE USE POLICY

As accepted by the Board 6/25/2014

PURPOSE

To better serve the public, and to provide our employees with the best tools to do their jobs, TJSWCD makes available to our workforce access to one or more forms of electronic media and services, including computers, e-mail, telephones, voicemail, fax machines, intranet and Internet. TJSWCD encourages the use of these media and associated services because they can make communication more efficient and effective and because they are valuable sources of information. However, all employees and everyone connected with the organization should remember that electronic media and services provided by the District are District property and their purpose is to facilitate and support District business. All computer users have the responsibility to use these resources in a professional, ethical, and lawful manner. To ensure that all employees are responsible, the following guidelines have been established for using electronic resources. No policy can lay down rules to cover every possible situation. Instead, it is designed to express TJSWCD's philosophy and set forth general principles when using electronic media and services.

PROHIBITED COMMUNICATIONS

Electronic resources cannot be used for knowingly transmitting, retrieving, or storing any communication that is: discriminatory or harassing; derogatory to any individual or group; obscene, sexually explicit or pornographic; defamatory or threatening; in violation of any license governing the use of software; or engaged in for any purpose that is illegal or contrary to TJSWCD policy or interests.

PERSONAL USE

The computers, electronic media and services provided by TJSWCD are primarily for business use to assist employees in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect either the systems' use for their business purposes, or the employee's ability to fulfill work responsibilities in a timely manner. However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

ACCESS TO EMPLOYEE COMMUNICATIONS

Generally, electronic information created and/or communicated by an employee using e-mail, word processing, utility programs, spreadsheets, voicemail, telephones, Internet and bulletin board system access, and similar electronic media is not reviewed by the District. However, the following conditions should be noted:

TJSWCD Acceptable Use Policy
Section IV.6 of Policy Manual

TJSWCD reserves the right to gather logs for electronic activities or monitor employee communications directly, e.g. telephone numbers dialed, sites accessed, call length, and time at which calls are made, for the following purposes: cost analysis; resource allocation; optimum technical management of information resources; detecting patterns of use that indicate employees are violating organization policies or engaging in illegal activity; and other training purposes.

TJSWCD reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other District policies. Employees should not assume electronic communications are completely private. Accordingly, if they have sensitive information to transmit, they should use other means.

SOFTWARE

To prevent computer viruses from being transmitted through the District's computer system, unauthorized downloading of any software is prohibited. Authorization to download a **free** program must be obtained prior to download from *either* the District Manager *or* Management Analyst. Authorization to **purchase** a program using District funds or to receive reimbursement from District funds must be obtained from *both* the District Manager *and* Management Analyst prior to purchase. TJSWCD may require that either the Management Analyst or a licensed computer technician from a contracted computer services company perform the installation of any software you request, more often in cases of free software or software that requires specialized configuration.

SECURITY

Employees must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been granted by District management, employees are prohibited from engaging in, or attempting to engage in: monitoring or intercepting the files or electronic communications of other employees or third parties; hacking or obtaining access to systems or accounts they are not authorized to use; using the log-ins or passwords of other employees; breaching, testing, or monitoring computer or network security measures; sending e-mail or other electronic communication designed to obscure or alter the representation of the sender; using copyrighted material, except as permitted by the copyright owner; and accessing external systems via botnet, rootkit, or other method with the intent of causing harm to another organization or individual.

PASSWORDS

Employees must maintain a hard-copy log of passwords used to access any TJSWCD-related systems, software, or web programs, including but not limited to: computer user accounts; TeamViewer or other remote viewing software used to access work devices; DCR Tracking; VRS Navigator for Employers; payroll administration software; online access to District bank accounts.

This log will be kept in the individual personnel files of the employees, located in the locking file cabinet #2 at the Management Analyst's desk. This log may only be viewed by the Chairman of the Board of Directors, District Manager, Management Analyst, or individual employee. Any request to view or remove the log from the file for any length of time must be noted in writing.

PARTICIPATION IN ONLINE FORUMS

Employees should remember that any messages or information sent on District-provided facilities to one or more individuals via an electronic network—for example, Internet mailing lists, bulletin boards, and online services—are statements identifiable and attributable to TJSWCD. Any opinions expressed through a TJSWCD communications device must be demarcated as follows:

"This personal opinion does not reflect the opinions, policies, views or beliefs of the Thomas Jefferson SWCD."

VIOLATIONS

Any employee who abuses the privilege of their access to e-mail or the Internet in violation of this policy will be subject to corrective action, including possible termination of employment, legal action, and criminal liability.