Thurston County Fire Protection District 8
DISTRICT POLICY MANUAL

POLICY TITLE:	Information Technology & Media
PROCEDURE NUMBER:	1-22
REVISION:	4
DATE ISSUED/REVISED:	**DRAFT**
BOARD APPROVAL:	

It is the District's policy to establish reasonable rules and regulations regarding use of electronic devices (whether District owned or owned by a member) and the content of electronic media generated or received on District property and generated or received by Members while engaged on District business. All members are responsible for proper use of District information technology and media (IT&M) devices and will be held accountable for any misuse or abuse of IT&M systems or information, either through the member's own actions or by the actions of others whom the member has allowed access. Members' use of social media is addressed in *District Policy 1-23 "Social Media & Imagery"*.

I. DEFINITIONS: for the purposes of this Policy, the following definitions shall apply:

1) DISTRICT BUSINESS PURPOSES - shall mean any work conducted by members directly or indirectly as part of their assigned District job duties as opposed to activities undertaken for personal business or other purposes.
2) ELECTRONIC (IT&M) DEVICES – shall mean any equipment or programs that are used for the purpose of sending and receiving electronic media. These may include but are not limited to computers, cell phones, fax machines, pagers, television/DVD, radio, or other portable media players.
3) ELECTRONIC MEDIA – shall mean any electronic communication that conveys a message, image, video, music, or any other communication form.

II. DISTRICT IT&M MANAGER: The Fire Chief shall appoint an IT&M Manager (District Secretary). The Fire Chief and IT&M Manger shall jointly:

1) Ensure that all District-owned IT&M Devices, related technology and software used by the District for electronic communications include reasonable protective measures to help prevent misuse or damage;
2) Manage the process of accessing information (including downloading information or software), virus detection and control, access controls, and related security mechanisms for use of the District's IT&M system(s); and
3) Ensure that the provisions of this Policy are maintained and enforced.

III. USE OF IT&M ASSETS: A minimal use of the District-owned IT&M Devices to communicate to other members non-District Business Purpose information is authorized as long as it does not violate the specific prohibitions listed below, is general in nature, distributed to the general membership or work group or is approved by the Fire Chief prior to being sent. Use of the District wireless network ("Wi-Fi") is specifically addressed in sub-section "E" below.

A--Specific misuse of the District-owned IT&M Devices includes, but is not limited to, the following:

1) Viewing, downloading and/or sending pornographic materials;
2) Sex-texting, soliciting sex, unwelcome sexual advances in any form to anyone;
3) Defaming members, citizens or any other person;
4) Marketing of personal or private business;
5) Transmitting or receiving material that would violate *District Policy 3-20 "Workplace Harassment"*;
6) Sending or posting confidential materials to unauthorized persons or places.
7) Using District time and resources for personal gain;
8) Sending or posting information that could damage the image or reputation of the District;
9) Promoting any political purposes including but not limited to ballot measures, political campaigns and lobbying issues;
10) Accessing, downloading, viewing or distributing of movies, music, software or any other materials protected by copyright laws without permission, or of the same containing or supporting any prohibited or illegal content or activity;
11) Uses that tend to compromise the safety or security of the public or public systems;
12) Uses that violate a legal ownership interest of any other party;
13) Use that accesses any service or facility that could incur service charges against the District and have not been previously authorized; and/or
14) Uses that constitute or encourage illegal activity.

B--Violations of this policy shall subject the member to discipline, up to and including termination. Refer to *District Policy 3-07 "Disciplinary Process"* for further information.

C--The IT&M Manager shall ensure that adequate protection is in place to prevent external tampering/hacking or invasion of viruses into the District's IT network. Members shall not connect any form of non-District transportable media to the District IT network without approval of the IT&M Manager and proper screening prior to launching of any content.

Any unauthorized modification to the District's IT network, IT&M devices, or any District owned hardware/software related to IT&M infrastructure, is prohibited; these action include (but are not limited to) a) adding unauthorized network switches, wireless access points, routers, fire-walls, network-attached storage devices or external hard-drives to the network; b) unauthorized disconnection of District IT network devices; c) plugging devices into the network in a manner to bypass the fire-wall without specific authorization, and/or d) unauthorized installation of software, utilities or operating system modifications. These modifications can affect the security and integrity of the system and is therefore a violation of District Policy.

D--Specific conditions for cellular telephone on-duty use include:

1) Whenever security or confidentiality concerns warrant use of a telephone rather than a two-way radio;
2) To conduct District business in some cases on a daily basis for command personnel;
3) Calls may be directed in to District cell phone equipped apparatus if necessary; and
4) While emergency services have been granted an exemption to laws covering "distracted driving", all efforts should be made to not talk on a cell phone while driving District vehicles unless utilizing hands free devices.

E--District wireless networking capability: as a benefit to its members and public using District facilities, the District provides wireless networking ("Wi-Fi") capability to access the Internet. All District wireless network traffic is not encrypted or guaranteed to be secure from interception; users should have up-to-date virus detection software installed on their wireless device. All wireless Internet access is subject to content filtering which will block access to prohibited Internet sites, including specifically those that contain adult content. The District prohibits use of its wireless network for uses that violate Section III (A) of this Policy.

IV. PUBLIC INFORMATION: Members recognize that any information entered, transmitted, received or stored on or through any District IT&M device is subject to inspection and monitoring by the District at all times. No member should expect that information they have entered, transmitted, received or stored shall be considered or treated as private or confidential . In any event, there are electronic records of the identity of the person entering, transmitting, receiving and/or storing information that may be open to public inspection without the consent of the parties at any time and without their consent. Information stored on a District IT&M device is the property of the District and may be considered a record subject to disclosure under the Open Public Records Act.

Release of public information shall be in compliance with *District Policy 1-20 "Public Access to District Records"* and *District Policy 1-91 "Public Information."*

V. PROCUREMENT, MAINTENANCE & DISPOSAL: Procurement, maintenance and disposal of IT&M Devices and assets shall comply with *District Policy 1-03 "Procurement, Expenditures & Audit General Guidelines"* and *District Policy 1-25 "Inventory of Assets."*