**Section 100 – Management & Administration**

|  |
| --- |
| General Rules & Administration - 100 |
| S.O.P # 100.25 | **Email & Electronic Equipment** | Page: 1 of 3 |
| EFFECTIVE: 10/14/2019 | Authorized: Board of Directors |
| REVISED: |  |

**100.25.01 Purpose**

The purpose of this SOP is to establish a policy concerning the use of District electronic equipment and the internet.

**100.25.02 General**

The District uses multiple types of electronic equipment, facilities and services for producing documents, research and communication including, but not limited to; computers, software, email, copiers, telephones, voicemail, fax machines, online services, cell phones (including text messages), the Internet and any new technologies used in the future. This policy governs the use of such District property.

**100.25.03 Ownership**

All information and communication in any format, stored by any means on or received via the District’s electronic equipment, facilities or services is the sole property of Jefferson County EMS District.

**100.25.04 Usage**

All of the District’s electronic equipment, facilities and services are provide and intended for District business purposes only and not for personal matters, communications or entertainment. Access to the Internet, web sites and other electronic services paid for by the District are to be used for District business. Incidental use of District property is allowed as approved by the Chief or Asst. Chief. Employees may not use District provided internet, or electronic equipment, facilities and services to:

* Display or store any sexually explicit images or documents, or any images or documents that would violate District’s no-harassment and no-discrimination policies;
* Participate in social media games or technology supported games;
* Engage in any activity that violates the rights of any person or company protected by copyright, trade secrets, patent or other intellectual property (or similar laws or regulations);
* Engage in any activity that violates the rights to privacy of protected healthcare information or other District-specific confidential information;
* Engage in any activity that would introduce malicious software purposefully into a workstation or network (e.g., viruses, worms, Trojan horses).
* Download or view streaming video for personal use. Streaming audio is allowed providing it does not contain explicit material, adversely affect network speed, or interfere with others’ ability to work.

Employees may not use JCEMSD-provided email addresses to create or manage personal accounts (e.g., shopping websites, personal bank accounts, and social media accounts).

The ROKU connected to the television in the sleeping area is for the crew’s enjoyment during down time. The District will pay for two different channels on the ROKU. These channels will be agreed upon by the staff collectively. No other channels will be added without the approval of the Chief.

**100.25.05 Inspection and Monitoring**

Employee communications, both business and personal, made using District electronic equipment, facilities, and services are not private. Any data created, received or transmitted using District equipment; facilities or services are the property of the District and usually can be recovered even though deleted by the user.

All information and communication in any format, stored by any means on District’s electronic equipment facilities or services, are subject to inspection at any time without notice. Personal passwords may be used for purposes of security, but the use of a personal password does not affect District’s ownership of the electronic information, electronic equipment, facilities, or services, or the District’s right to inspect such information. The District reserves the right to access and review electronic files, documents, archived material, messages, email, voicemail and other such material to monitor the use of all of the District’s electronic equipment, facilities and services, including all communications and internet usage and resources visited. The District will override all personal passwords if it becomes necessary to do so for any reason.

**100.25.06 Personal Hardware and Software**

Employees may not install personal hardware or software on District’s computers systems without approval from the Chief or Asst. Chief. All software installed on District’s computer systems must be licensed. Copying or transferring of District-owned software may be done only with the written authorization of the Chief or Asst. Chief.

**100.25.07 Unauthorized Access**

Employees are not permitted unauthorized access to the electronic communications of other employees or third parties unless directed to do so by the District’s management. No employee can examine, change or use another person’s files, output or user name unless they have explicit authorization from the Chief or Asst. Chief.

**100.25.08 Security**

Many forms of electronic communication are not secure. Employees who use cell phones, cordless phones, fax communications or email sent over the internet should be aware that such forms of communication are subject to interception and these methods of communicating should not be used for privileged, confidential, or sensitive information unless appropriate encryption measures are implemented.

**100.025.09 Inappropriate Web Sites**

The District’s electronic equipment, facilities or services must not be used to visit internet sites that contain obscene, hateful or objectionable materials, or that would otherwise violate JCEMSD’s policies on harassment and discrimination.