Subject:	**COMPUTER USE POLICY**
Section:	**PPG# 3350.4**
Chapter:	**Community Relations**
Effective Date:	**8/14/03**

1.0 POLICY

1.1 McLane/ Black Lake Fire Department is committed to protecting our members, the patients we serve, and the department from illegal or damaging actions by individuals and the improper release of protected health information and other confidential information.

1.2

Confidential information shall be protected at all times, regardless of the medium by which it is stored or transmitted. Examples of confidential information include but are not limited to: individually identifiable health information concerning patients, department financial and business information, patient lists and reports, and research data. Department members shall take all necessary steps to prevent unauthorized access to this information.

1.3

This policy applies to employees, volunteers, members, contractors, consultants, temporary employees, students, and others at McLane/ Black Lake Fire Department who, have access to computer equipment, including all personnel affiliated with third parties.

1.4

This policy applies to all equipment that is owned or leased by McLane/ Black Lake Fire Department and includes equipment provided by South Puget Sound Community College in use in District facilities.

1.5

Any member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or membership.

2.0 GUIDELINES

2.1 Use and Ownership of Computer Equipment

2.2 All data created or recorded using any computer equipment owned, controlled or used for the benefit of McLane/ Black Lake Fire Department is at all times the property of McLane/ Black Lake Fire Department. Because of the need to protect McLane/ Black Lake Fire Department's computer network, the company cannot guarantee the confidentiality of information stored on any network device belonging to McLane/ Black Lake Fire Department, except that it will take all steps necessary to secure the privacy of

all protected health information in accordance with all applicable laws.

2.3 The District also makes available computers owned by South Puget Sound Community College to assist fire protection technology students in the pursuit of knowledge and academic development. These resources shall only be used for academic assignments and authorized education and research.

2.4 Fire Protection Technology Students shall also abide by the provisions of South Puget Sound Community College, Computer Resources Acceptable Use Policy.

2.5 Members are responsible for exercising good judgment regarding reasonable personal use and must follow operational guidelines for personal use of Internet/Intranet/Extranet systems and any computer equipment.

2.6 At no time may any pornographic or sexually offensive materials be viewed, downloaded, saved, or forwarded using any Company computer equipment. Please refer to *Policy and Procedural Guideline #2102, Workplace Harassment*.

2.7 For security and network maintenance purposes, authorized individuals within McLane/ Black Lake Fire Department may monitor equipment, systems and network traffic at any time, to ensure compliance with all department policies.

2.8 Rules governing electronic mail and internet usage apply to ALL computer equipment used while on department property. This includes privately owned equipment.

2.9 Under no circumstances is a member of McLane/ Black Lake Fire Department authorized to engage in any activity that is illegal under local, state or federal law while utilizing McLane/ Black Lake Fire Department's computer resources.

2.10 **Security and Proprietary Information**

2.11 Authorized users are responsible for the security of their passwords and accounts.

2.12 All PCs, laptops, workstations and remote devices should be secured with a password-protected screensaver, wherever possible, and set to deactivate after being left unattended for ten (10) minutes or more, or by logging-off when the equipment will be unattended for an extended period.

2.13 All computer equipment used by department members, whether owned by the individual member or McLane/ Black Lake Fire Department, shall regularly run approved virus-scanning software with a current virus database in accordance with company policy.

2.14 Members must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses.

2.15 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

2.15.1 Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by McLane/ Black Lake Fire Department.

2.15.2 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which McLane/ Black Lake Fire Department or the end user does not have an active license is strictly prohibited.

2.15.3 Exporting system or other computer software is strictly prohibited and may only be done with express permission of management.

2.15.4 Introduction of malicious programs into the network or server (e.g., viruses, worms, etc.).

2.15.5 Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

2.15.6 Using a McLane/ Black Lake Fire Department computer device to actively engage in procuring or transmitting material that is in violation of the department's prohibition on sexual and other harassment.

2.15.7 Making fraudulent statements or transmitting fraudulent information when dealing with patient or billing information and documentation, accounts or other patient information, including the facsimile or electronic transmission of patient care reports and billing reports and claims.

2.15.8 Causing security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the staff member is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.

2.15.9 Providing information about, or lists of, McLane/ Black Lake Fire Department members or patients to parties outside McLane/ Black Lake Fire Department.

2.15.10 E-mail and Communications Activities

2.15.11 Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).

2.15.12 Any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages.

2.15.13 Unauthorized use, or forging, of e-mail header information.

2.15.14 Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.

2.15.15 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

2.15.16 Use of unsolicited e-mail originating from within McLane/ Black Lake Fire Department networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by McLane/ Black Lake Fire Department or connected via McLane/ Black Lake Fire Department's network.

Use of Remote Devices

2.16 The appropriate use of Laptop Computers, Personal Digital Assistants (PDA's), and remote data entry devices is of utmost concern to McLane/ Black Lake Fire Department. These devices, collectively referred to as "remote devices" pose a unique and significant patient privacy risk because they may contain confidential patient, member or department information and these devices can be easily misplaced, lost, stolen or accessed by unauthorized individuals

2.17 Remote devices shall not be used for department business without prior department approval.

2.18 McLane/ Black Lake Fire Department must approve the installation and use of any software used on the remote device.

2.19 Remote devices containing confidential or patient information must not be left unattended.

2.20 If confidential or patient information is stored on a remote device, access controls must be employed to protect improper access. This includes, where possible, the use of passwords and other security mechanisms.

2.21 Remote devices containing confidential or patient information shall only be used by authorized users.

2.22 Remote device users will not install any software onto any PDA owned by McLane/ Black Lake Fire Department except as authorized by McLane/ Black Lake Fire Department.

2.23 Users of department-owned remote devices will immediately report the loss of a remote device to a supervisor or the Privacy Officer.

2.24

3.0 REFERENCES

3.1 Health Insurance Portability and Accountability Act of 1996 (HIPPA).