ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES

LOGAN TOWNSHIP FIRE SERVICE
SUGGESTED OPERATING PRACTICES

Date: 11/6/2008 Revision Date: Section:

PURPOSE:
To establish a policy regarding the acceptable use of Information Technology Resources for Logan Township Fire Service members and volunteers.

RESPONSIBILITY:
It is each individual's responsibility to comply with this policy. Failure to do so will result in disciplinary action, up to and including termination.

PROCEDURE:
This is the Logan Township Fire Service's "Acceptable Use Policy" (AUP). Please read the policy carefully. While our direct connection to the Internet offers an array of potential benefits, it can also open the door to some significant risks to our data and systems if we do not follow appropriate security discipline. A computer systems user can be held accountable for any breaches of security or confidentiality resulting from his/her use of the Departments information resources or Internet connection.

The Logan Township Fire Service information technology systems provide access to the vast information resources of the Internet to help you do your job, provide software resources, and complete applicable forms and reports related to the fire service. The facilities that provide access represent a considerable commitment of Department resources for networking, telecommunications, software, storage, etc.

This AUP is designed to help you understand our expectations of the use of those resources and help you use those resources wisely.

While we have set forth explicit requirements for computer and Internet usage below, we would like to start by describing our AUP philosophy. First and foremost, the computers and Internet connection provided by this Department are business tools provided to you at significant cost. That means the Department expects you to use your computer access for Department-related purposes (i.e., to complete reporting, communicate with other fire/EMS agencies, citizens, to research relevant topics and obtain useful Department-related information), except as outlined below. We insist that you conduct yourself honestly and appropriately on the computer system, and respect the copyright, software licensing rules, property rights, privacy and prerogatives of others, just as you would in any other business dealings. All existing Department policies apply to your conduct on the computer system and Internet, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of Department resources, sexual harassment, information and data security, and confidentiality.

Unnecessary or unauthorized computer usage causes network and server congestion. It slows other users, takes away from work time, consumes supplies, and ties up printers and other shared resources. Unlawful computer usage may also garner negative publicity for the Department and expose the individual fire departments to significant legal liabilities.

The chats, newsgroups, and e-mail on the Internet give each individual computer user an immense and unprecedented reach to propagate the Department messages and tell our story. Because of that power we must take special care to maintain the clarity, consistency, and integrity of the Departments corporate image and posture. Anything any one individual writes in the course of acting for the Department on the Internet could be taken as representing the Department's corporate posture. The guidelines below are, in part, to ensure that any and all communications which could be attributed to the Department are appropriate.

While our connection to the Internet offers numerous potential benefits, it can also open the door to some significant risks to our data and systems if we do not follow appropriate security discipline. As presented in greater detail below, that may mean preventing machines with sensitive data or applications from connecting to the Internet entirely, or it may mean that certain users must be prevented from using certain

Internet features. The overriding principle is that security is to be everyone's first concern. Department members can be held accountable for any breaches of security or confidentiality.

DETAILED AUP PROVISIONS:

A. Definitions. For purposes of this policy, terms used should be interpreted expansively to include related concepts.

(1) *"Internet"* includes the Department's in-house system, the World Wide Web, and e-mail.

(2) *"Department"* refers to The Logan Township Fire Service as a whole, the five individual Logan Township Fire Departments, and the Logan Township Volunteer Fireman's Relief Association either collectively and independently.

(3) *"Department Equipment"* includes the Department's computer hardware, software, facilities, network, Internet facilities, services, and all other computing resources provided either locally or remotely.

(4) *"Electronic Communication"* shall mean any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic, or photo optical system. This term includes the so-called HTML files read in an Internet browser, any file meant to be accessed by a word processing or desktop publishing program or its viewer, or the files prepared for the Adobe Acrobat reader and other electronic publishing tools.

(5) *"Graphics"* includes photographs, pictures, animations, movies, or drawings.

(6) *"Display"* includes monitors, flat-panel active or passive matrix displays, monochrome LCDs, projectors, televisions, and virtual-reality tools.

(7) *"User"* includes any Department member.

(8) "*Network Management Team*" is the identified committee of personnel that are appointed by the Fire Chiefs Association and the Logan Township Volunteer Fireman's Relief Association to manage the Logan Township Fire Service Information Technology systems.

B. No Expectation of Privacy.

(1) Department Equipment shall be used for Department business and is not for personal use, with limited exception as set forth herein. Because Department Equipment can only be used for Department business, the Department considers itself to be a party to any communication utilizing Department Equipment.

(2) The Department has the right to access, monitor, and intercept any Electronic Communication during transmission where the Department is a party to the communication, and shall have such right where an employee of the Department is a party and has given the Department prior consent of such access, pursuant to the Electronic Communications Privacy Act, 18 U.S.C.A. § § 2510 to 2522 (1997).

(3) As the provider of the Department Equipment and related Electronic Communication services used by the employees of the Department, the Department shall have access to all Electronic Communications stored on the Department Equipment, pursuant to the Stored Wire and Electronic Communications Act, 18 U.S.C.A. § § 2701 to 2711 (1997).

(4) As a result of the above, no employee of the Department shall have any expectation of privacy with respect to Electronic Communications transmitted, received or stored on, by or through the Department Equipment. The Department will review activity and analyze computer usage patterns. It may choose to publicize this data to assure that Department computer resources are devoted to maintaining the highest levels of productivity.

(5) The Department retains the rights to any material posted to any forum, newsgroup, chat room or World Wide Web page by any member or volunteer using Department Equipment.

(6) Any software or files downloaded via the Internet into the Department network is the property of the Department. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.

C. Personal Use.

(1) Users of Department Equipment are expected to exercise good judgment and ensure that all Electronic Communications are appropriate, professional and courteous, and not in violation of any Department policy, or of any local, state, or federal law. The Department will not exercise editorial control by assuming responsibility to seek out and eliminate defamatory, obscene, or incidental materials; however, if such Electronic Communications, either during transmission or as stored on Department Equipment, comes to the Department's attention, the individual responsible shall be subject to discipline pursuant to the rules and procedures of the Department. The Department does not assume responsibility to exercise editorial control over any of the content of Electronic Communications and shall not act as a "publisher" of such materials.

(2) Because a wide variety of materials may be considered offensive by colleagues, citizens, or suppliers, it is a violation of Department policy to store, view, print, or redistribute any document or graphic file that is not directly related to the user's job or the Department's business activities.

(3) Employees with Internet access must take particular care to understand the copyright, trademark, libel, slander, and public speech control laws of all countries, so that personal use of the Internet does not inadvertently violate any laws, which might be enforceable against the Department.

(4) Computers may be used for personal interest on a limited basis, as described below. In some instances, Department Equipment may be provided to an employee for use in the home or outside of Department facilities. Personal use of Department Equipment is subject to the following conditions:

a. Personal use of Department Equipment shall not interfere with the operations of the Department. Department Equipment shall not be used to promote political agendas or to obtain any financial gain or avoid financial detriment that would otherwise not be available but for the employee's position. It is recognized, however, that due to the nature of the fire service schedules, limited personal use of Department Equipment is allowed. To the extent that expenses are incurred by the Department for personal use, the Department shall be promptly reimbursed for such expenses at the rate such services are generally available to the public, regardless to the actual cost to the Department.

b. While on station, users may utilize computer resources to prepare applications for desired Department positions, to type a social letter, prepare educational documents, play computer games described below, and Department-related course work.

c. In the interest of keeping employees well-informed, use of Internet news briefing services is acceptable while on station.

d. No user may utilize Department computer resources to maintain personal financial records, operate an outside business, or participate in any malicious activities.

e. Internet games and Personal games may not be loaded on Department systems. This included Internet based games or activities where files need to be installed onto the Department computer to allow the games to run. Games that come with the Windows operating system may be used. Department owned or licensed games created to teach knowledge or skill needed for Department positions may be used.

(5) Electronic communications will not contain offensive material. It is prohibited to transmit any inflammatory material; material with abusive language; sexually, culturally, or racially offensive or insulting material; or obscene, vulgar, or profane materials.

(6) The display of any kind of sexually explicit image or document on any Department system is a violation of Department sexual harassment policies. In addition, sexually explicit material may not be archived, stored, distributed, edited, or recorded with Department Equipment.

(7) The Department may use independently supplied software and data to identify inappropriate or sexually explicit Internet sites or e-mail. The Department may block access from within Department networks to all such sites known. If a Department user accidentally connects to a site that contains sexually explicit or offensive material, he or she must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program.

D. General Guidelines.

(1) Department Equipment must not be used to violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province, or other local jurisdiction in any material way. Use of any Department resources for activity illegal under the laws of any jurisdiction is grounds for immediate loss of membership, and the Department will cooperate with any legitimate law enforcement and/or prosecutorial activity.

(2) Department Equipment may not be used to download or distribute pirated software or data.

(3) Department Equipment may not be used to propagate any virus, worm, Trojan horse, or trap-door program code.

(4) Department Equipment may not be used to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

(5) Each user of Department Equipment shall identify him or herself honestly, accurately, and completely (including one's Department affiliation and function where requested) when participating in chats, conference, or newsgroups, or when setting up accounts on outside computer systems.

(6) Only those users who are authorized to speak to the media at public gatherings on behalf of the Department may speak/write in the name of the Department to any newsgroup, conference, or chat room. Other users may participate in newsgroups or chats in the course of business when relevant to their duties, but they do so as individuals speaking only for themselves. Where an individual participant is identified as a volunteer of this Fire Department, the member must refrain from the unauthorized endorsement or appearance of endorsement by the Department of any commercial product, political position or candidate.

(7) Users are reminded that chats and newsgroups are public forums where it is unlawful to reveal confidential Department information, including patient data. Users releasing such confidential information via a newsgroup or chat, whether or not the release is inadvertent, will be subject to discipline as per the departments SOP's.

(8) Use of Department Equipment to commit infractions such as misuse of Department assets or resources, sexual harassment, unauthorized public representation of Department, and misappropriation of intellectual property is prohibited by Department procedures and will be sanctioned under the relevant provisions of the respective governing SOP's.

(9) Members using Department Equipment with Internet access may download only software with a direct business purpose and must arrange to have such software properly licensed and registered. Downloaded software must be used only under the terms of its license.

(10) Members with Internet access may not use Department Equipment to download images or videos, unless there is an express business-related use for the material.

(11) Members with Internet access may not upload any software licensed to the Department or data owned or licensed by the Department without the prior written permission of the Network Management Team.

E. Technical.

(1) Any downloaded file must be scanned for viruses before it is run or accessed.

(2) The Department will maintain keys, combinations, and passwords to all computer hardware, software, and information created and/or stored on Department provided systems. All such information created and/or stored on these systems shall be considered Department property and is subject to inspection. Personal computer programs are not to be installed or used on Department computers without prior written permission of the Network Management Team.

(3) No privately owned device may be connected to Department Equipment, registered to the department domain, or connector to Department phone lines without prior written authorization of the Network Management Team. The exception would be if there are specific provisions made for such connections. i.e. Wireless access made available for general use of private laptops, ect.

(4) Users may encrypt their e-mail and files with the use of software with prior written authorization of the Network Management Team.

F. Security.

(1) Department Equipment is protected from unauthorized access and use by passwords and other security measures. The security measures recognize that information is exempt from Public Record Disclosure, and that the integrity of the business of the Department must be safeguarded. All users are advised that the use of a password does not give rise to any right of privacy, and that passwords must not be disclosed to unauthorized users. Users also are advised that the use of the deletion keystroke does not necessarily mean that a record, communication, or document has been eliminated from the system.

(2) User ID's and passwords help maintain individual accountability for computer resource usage. Any user who obtains a password ID for a computer resource from the Department must keep that password confidential. No one should use the ID or password of another, nor should anyone provide his or her password to another. The user may need to work with the Network Management Team to troubleshoot problems from time to time, but if the user's password is shared in the course of this process, the user

should immediately change such passwords to regain the exclusive knowledge of same. The Network Management Team will be responsible for setting up and tracking of user accounts and system operation and configuration. The Network Management Team shall be the only group authorizing system or configuration changes to Department owned and operated equipment.

(3) The Department has installed an Internet firewall to assure the safety and security of the Department's network. Any user who attempts to disable, defeat, or circumvent any Department security facility will be subject to immediate loss of membership.

(4) Only those Internet service and functions with documented purposes for this Department will be enabled at the Internet firewall.

(5) Whenever a user is done using the computer resource for a particular session, he or she shall always logout of all systems to be sure to maintain system and user security.

(6) All users will be required to maintain a password of a certain complexity and will be required to change this password at a pre-determined interval to ensure and maintain system security.

G. Obtaining Access.

(1) Department members or volunteers wishing to obtain a user account will contact their department IT representative and supply the required information needed to create an account. All users will be required to sign and return an acknowledgement sheet that they received and understand the Logan Township Fire Service AUP for Department IT resources. Once the Department IT contact has this form, they will provide instructions, a username, and temporary password for the user to access the IT systems.

(2) The Department IT Team will routinely evaluate the need for user's access and disable accounts with no activity, or members no longer associated with the fire service.

END OF POLICY

ACKNOWLEDGMENT

I, _____, acknowledge that I have received a written copy of the Logan Township Fire Service Acceptable Use Policy. I understand the terms of this policy and agree to abide by them. I understand that the Department may record and store for management use the electronic communications I send and receive, the Internet address of any site that I visit, and any network activity in which I transmit or receive any kind of file while using or connected to a Department computer or resource. I also understand and consent to the Department's right to access, monitor, and intercept any electronic communication to which I am a party during transmission. I understand that any violation of this procedure could lead to my discipline, including dismissal from the Department and criminal prosecution.

_____

Signature Date

_____

Name (printed) Station

This form must be signed and returned before any user access will be enabled. This form will be returned to and kept on file by the Logan Township Fire Service IT administrators.