Social Media & Internet Usage

Social Media

&

Internet Usage

Kyle Kaufman

Florence Fire/EMS

Personnel Management, 20FST481

Instructor Lawrence Bennett

March 2011
CERTIFICATION STATEMENT

I certify that this paper for my applied research project is my own work. This paper is respectfully submitted to my instructor for Personnel Management, Lawrence Bennett. This paper is submitted in March of 2011 as a required assignment for the listed course through the University of Cincinnati, OH. In the event that the language or writing of another individual is used, it shall be properly indicated and credited to the source.

Kyle N Kaufman
ABSTRACT

This research project was conducted because of the wide availability of the Internet and the increase in social media. The problem is that most public employees lack guidance from their employer on what is or is not appropriate conduct in these forums. Their conduct, at work and outside of work, can reflect directly on the employer. The project reviewed some employee and employer rights and some policies and guidelines of three different organizations related to internet usage. The method used for this project was historical research to produce an action type result. Based on this research a sample standard operating guideline was developed and included in the appendix. Also included in the appendix are guidelines on Internet usage from two of the organizations. It is recommended that employers develop some type of policy or guideline that reflects their mission, professionalism, and ethics and the use of social media. The employer should also train their employees on this policy in order to create a fair work environment. With a policy and knowledgeable employees, hopefully inappropriate use of social media can be avoided. This can protect both the employee and the employer.
TABLE OF CONTENTS

Title Page ........................................................................................................................................ 1
Certification Statement ....................................................................................................................... 2
Abstract ............................................................................................................................................... 3
Table of Contents ................................................................................................................................ 4

Main Body

Introduction .......................................................................................................................................... 5
Background and Significance ............................................................................................................... 5
Literature Review ................................................................................................................................. 7
Procedures .......................................................................................................................................... 10
Results ................................................................................................................................................ 11
Discussion .......................................................................................................................................... 12
Recommendations ................................................................................................................................. 13
Reference List ....................................................................................................................................... 15
Appendix ............................................................................................................................................. 16
INTRODUCTION

Are policies or guidelines needed within public service departments to guide employee participation in social networking and social media type activities on the Internet? Without guidance, employees will be left on their own to decide what level of appropriateness some information may be to their employer, or how private some information should be. The following research and recommendations should lead to a better understanding of employee and employer rights and why having policies or guidelines may be beneficial to both parties. Through a review of the current situation the needs for the future should be determined.

BACKGROUND AND SIGNIFICANCE

As the Internet has gained popularity over the years, so has social media. These sites allow users to have profiles, blog, be seen in pictures, use message boards, be associated with organizations, employers or other groups, and be linked to other associates or friends. These sites are continuing to expand the different ways in which they can be used. Some of the most commonly known sites are Facebook, MySpace, and Twitter. However, other sites are available and new ones will most likely emerge. Even Facebook, MySpace, and Twitter have only existed since 2004, 2003, and 2006 respectively, but membership availability has changed in short years and some of the sites existed under different names targeting different membership groups prior to their current creation date.

Many public employers have policies relating to professionalism and ethical conduct that are aimed at achieving the mission of the agency. These professionalism and ethical conduct policies should equally extend to use of social media where the employee can be associated with their employer. In this technology driven age, the use of the Internet and email communications are commonplace and often supported by employer systems. Some employers may go so far as
to define what they view as acceptable and unacceptable use of their electronic systems. These systems are in place and available to aid in the employees ability to effectively do their job. An employer may restrict their use and monitor their employees.

Professional organizations often network in order to further the expansion of their organization and to maintain an awareness of updates or changes in industry standards that relate to their type of business. Employers may even pay for membership fees associated with networking or foster an environment that encourages networking or attending conferences. With the growth of social networking available on the Internet, many professional organizations are able to continue and expand this networking in a cost effective manner considering they generally already have Internet access available to them. Public agencies have even joined in the networking; they realize the need to give people an easy and comfortable way to communicate with the agency. It also aids in the ability to disseminate information to large numbers of people quickly if their target population is using the same form of social media networking and they are linked to each other. Organizations may even encourage employees or members to become part of these social networks to further their cause or make themselves more accessible to the general public. Employees must be aware that while their participation may be allowed or even encouraged that they must still be conscientious of the impact that their profiles, pictures, posts, comments, or other information may have on their employer.

Employees generally have an expectation and a right to privacy. However, the employee must recognize that their privacy may have limits. Participation in networking by an employee that is not supported by the employer can still have an impact on the employer if the employee openly portrays himself or herself as a member of that organization or is readily identifiable because of their profile, pictures, or comments. Depending on policies the employer has in place,
it may not matter whether the employee’s participation took place through their systems or whether or not they were at work, on duty, or being paid.

Considering it is now commonplace for individuals to have phones with Internet access on them almost continuously, the likelihood of the Internet and these social media formats expanding is almost certain. Policies or guidelines related to social media, networking, and Internet usage could easily express an employer’s expectations more explicitly than just applying general professionalism and ethical conduct policies. They could offer protection to both the employer and employee should a conflict arise.

**LITERATURE REVIEW**

*Internet Manual*

In 2010, the International Association of Fire Fighters (IAFF) published a manual titled, *The Law and the Internet for IAFF Affiliates*. Within this manual, the issue of an individual’s First Amendment rights are covered in detail. The First Amendment of the Constitution is part of the Bill of Rights. It protects individuals from having laws passed that restrict their freedom of speech. It should be noted that private employers are allowed to restrict their employee’s speech. Employees within the private sector have an inherent right to their freedom of speech, but employers can discipline them, separate them from employment, or bring charges against them if their speech is not useful or destroys their value.

Public employers cannot arbitrarily restrict their employee’s speech. “When the state acts as an employer, rather than as a sovereign, the courts have recognized that the employer possesses a limited interest in regulating the speech of its employees” (IAFF, 2010, p. 9); as seen in the decision of *Pickering v. Board of Education*. Public employers need to have the ability to hold their employees accountable for the things that say and do regardless of whether they are at
work or off. The IAFF provided the following citation from *Waters v. Churchill*; “When someone who is paid a salary so that she will contribute to an agency’s effective operation begins to do or say things that detract from the agency’s effective operation, the government employer must have some power to restrain her.” (2010, p. 9)

When a public employee is speaking in their official capacity, they are not granted First Amendment protection. Otherwise, the manual goes on to describe how to determine whether a public employee’s speech is protected. First, is the subject matter of the speech of public concern? If it is not, then there is not First Amendment protection. If the matter is of public concern, the employee’s personal interest in speaking on the subject matter must be weighed against the harm or interruption to the public employer’s operations.

Another issue that the Internet manual covers is privacy. The Fourth Amendment protects individuals from unreasonable search and seizures by the government. Electronic devices and system usage are generally not protected if they are owned by the governmental agency and they have policies relating to the monitoring that the employee has been notified about. The use of personal devices and access to personal accounts is protected as long as the employee’s use is not related to any work-related misconduct and the employee takes actions to prevent use or viewing by other employees. However, using personal devices on an employer’s network may be monitored in the same way that the employer monitors devices of their own. Simply bringing a personal electronic device to work does not cause a loss in an employee’s right to privacy.

The IAFF also answers questions regarding using sites such as *Facebook, MySpace,* and *Twitter.* The IAFF suggests that there should be no expectation to privacy by the employee that posts information. Employees should take advantage of any available privacy control setting available to them on any social site that they choose to use.
City of Florence Policies

The City of Florence is the governing body for the Florence Fire/EMS Department. Florence is located on the eastern border of Boone County, KY. Within their personnel policies for the City is a section on city business systems. These systems include computers, phones, software, email, and Internet. The personnel policy addresses the issue that there should be no expectation of privacy for all information transmitted through or stored on their systems. Email and Internet access is intended to facilitate job functions. Personal use should be limited and is subject to their other requirements. Per the City’s personnel policies, “access and use of Internet-based, third party e-mail systems (e.g., Hotmail, Yahoo, MSN) via the City network should be kept to a minimum.” (Florence, 2010, p. 15) The City will monitor all city business systems. The City expresses the fact that you are representing them when using the Internet.

The City of Florence also has an administrative procedure approved by executive order regarding computer use. Administrative Procedure No. 3, City of Florence Computer Use Procedure, is more detailed than the personnel policies. In addition to the personnel policies, the procedure requires that employees and volunteers sign a “Computer User Memorandum of Agreement”. The procedure also prohibits the use of personal or non-City owned hardware on the City’s network without their approval. Per the City’s administrative procedure, “access to Internet-based, third party e-mail systems (e.g., Hotmail, Yahoo, MSN) via the City’s network is prohibited.” (Florence, 2006, p. 5)

Burlington Fire Protection District SOG

Burlington Fire Protection District is a combination department that services part of central Boone County, Kentucky. They have a standard operating guideline (SOG) that refers to electronic mail and Internet usage, SOG #400.13. It is specific to electronic mail and Internet
usage within their stations. It identifies that their electronic mail and Internet usage is for the purposes of conducting official business and completing assigned responsibilities. A certain amount of personal email is permitted, but “personal messages should be kept to a minimum.” (Burlington, 2003, p. 1) It does acknowledge, “e-mail is not privileged communication, nor subject to privacy.” (Burlington, 2003, p. 1) The District does have the right to monitor usage by the individual user accounts.

**Gum Branch Fire & Emergency Services SOG**

Gum Branch Fire & Emergency Services is a 100% volunteer organization in Liberty County, Georgia. Gum Branch does not currently have Internet access at its station, but they still have a policy to cover its usage should it become available. They also recognize that the policy would need to be updated if access became available. Gum Branch wants its member to recognize that they represent the department when they use the Internet and that personal email accounts will not be accessed while at the station. They also identify that messages are property of the department.

**Procedures**

A historical review of the literature was completed in order to produce the following results. Information was gathered from the City of Florence, the IAFF, Burlington Fire Protection District, and online from Gum Branch Fire & Emergency Services. Reviews of the policies and SOGs led to the development of the sample SOG provided as a result. While gathering and reviewing the literature is fairly objective, the levels to which the policies and SOGs are enforced and the current acceptable practices within the respected organizations are more subjective. These subjective aspects are not covered in this research project. This research project has been limited to literature reviewed; additional literature could also be reviewed.
RESULTS

As seen in the IAFF Internet manual, consideration must be given to employee rights. Public employers have a more difficult time regulating their employee’s speech than a private sector employer. Speech is often protected if it is a matter of public concern and the employee’s interest in speaking outweighs the effect on the employer operations. Employers must also recognize that employees do have certain privacy rights when it comes to their personal hardware or accounts that exist outside their place of employment. If an employed wishes to monitor employee’s usage of their systems, they must develop policies and ensure that their employees are notified of the policies.

All three of the organizations whose policies were reviewed made mention of employees having no expectation of privacy while using their systems or the fact that all information sent is the organization’s property. Gum Branch and Florence identified that the employee is a representative of the organization, even in email and Internet usage. Florence and Burlington both have policies on monitoring usage. Of the three organizations, Florence has the most extensive policies regarding their systems. Florence includes the signing of a user memorandum and addresses the use of non-city owned hardware. Florence, like Gum Branch, addresses personal email and third-party email providers, but Florence’s personnel policies and administrative procedure differ in that one strictly prohibits access and the other allows for minimal usage.

The IAFF specifically addressed social media, but none of the three organizations reviewed addressed the issue. A quick search of Facebook found that the City of Florence and the Florence Professional Fire Fighters Local 3303 both had Facebook pages. Nothing was found on Facebook, MySpace, or Twitter for the other two reviewed organizations. While the individual
organizational needs should always be identified prior to developing policies or SOGs, a sample SOG regarding social media is included in the appendix. The SOG is basic, but could provide a starting point for an organization. Also included in the appendix along with the SOGs from Burlington Fire Protection District and Gum Branch Fire & Emergency Services are included in the appendix.

**DISCUSSION**

Every organization will have slightly different needs and expectations. However, most of their needs and expectations will be similar. Public safety organizations have a need to operate efficiently and have resources available to their personnel. They will expect their personnel to represent them in a professional and ethical manner without discrediting or tarnishing the image and operations of the organization.

Some public organizations take a fairly strict stance towards the use of their business systems, such as the City of Florence. Others have no written policies regarding their systems. It is apparent that organizations already recognize that their employees reflect on their organization. They explicitly say this in their policies, and it should be recognized that an employee still represents their employer even when they are off-duty. One policy cannot be written that would cover every organization. While one employer may be strictly ruled and overseen by their employment board, another may be trying to facilitate an atmosphere that draws people to the organization by creating a more homelike environment with less strict rules. Some public employers may feel that since their business systems are paid for by public funds, that their use should be for official business only. A volunteer organization may view unmonitored Internet use as an incentive to keep volunteers at the station. Some departments may view Internet usage different depending on the time of day, such as during normal business
hours versus “down-time”. (“Down-time” being periods of time where an employee of a public safety organization may not be assigned other tasks beyond the responsibility to respond to requests for service.) However, Internet usage, like almost anything, could be a liability. In order to manage this liability, guidance should be given.

Internet usage outside the workplace can have a great impact on the work environment also. The use of social networking sites is popular, and employers should consider giving guidance to their employees in order to protect both the employee and employer. Social networking sites could also be the media used to harass an employee. Even if the comments are posted away from work, if it creates a hostile working environment the employer could end up involved in litigation if the situation is not handled appropriately. It may be easier to make an attempt to prevent the situation rather than only being reactive to other’s actions.

Having policies or guidelines can benefit both the employer and the employee. Employees will benefit by having rules to follow and knowledge of the expectations of the employer. The employer can benefit by having less problems to deal with and having an outline to follow to easily decide if an employee’s actions were inappropriate.

**Recommendations**

Public employers should not ignore the issue of social media and Internet usage. Some policy or guideline should be written. Policies and guidelines should not contradict each other, as this could create confusion or different enforcement practices.

Employers could consider the use of a committee to make recommendations for the development or update of social media and/or Internet usage policies. The employer should educate the committee of any boundaries prior to them meeting and making recommendations. Otherwise their recommendations may be outside of what management is willing to consider. If
management would not be willing to consider their recommendations, then forming a committee would be counter-productive. If there is a collective bargaining agreement between the employer and the employees, it may be appropriate to incorporate some type of policy or understanding within the agreement.

Regardless of the depth of an employer’s policy or guideline, the employer should be sure to educate their employees. They should be educated on their rights as employees, what rights the employer has, what policies and practices exist, and the employer’s expectations. To protect the employer, they should maintain records of the training and notifications that they make to their employees.
REFERENCES

Burlington Fire Protection District. (2003). SOG #400.13 *Electronic Mail (E-mail) and Internet Usage*. Burlington, KY: Author


APPENDIX

Appendix A: Sample SOG

Appendix B: Burlington Fire Protection District SOG #400.13

Appendix C: Gum Branch Fire & Emergency Services Information Security Policy
Appendix A
Sample Agency Name

SOG #100

Social Media

Last Revision: 3/1/11
Next Review: 3/1/13

Purpose
To establish a guideline for the use of social media.

Introduction
Many forms of social media are currently available, such as Facebook, MySpace, and Twitter. It is not the intent of this agency to determine whether or not you should participate in any type of social media, but rather to provide guidance for those who do choose to participate.

Scope
The administration will be responsible for updating this guideline. The guideline will apply to all members of the agency, including, but not limited to: volunteers, paid staff, associate members, and administrative positions. The administration will be responsible for notifying all members of the guideline, any updates, training, and maintenance of forms regarding notification and understanding of the members. All members are responsible for following the guideline and notifying supervisors if they are aware of someone not following the guideline. Members may be subject to disciplinary action as set forth in applicable policies and guidelines related to discipline.

Guideline
Social media includes any type of Internet or technology based application that allows the exchange of information that can be generated by users.

Members using social media should be aware that information is generally not private. Any available privacy controls to restrict public view should be used.

Members should not post content that is of questionable nature when compared to the agency's mission statement, code of ethics, or professionalism policy. Members should be aware that even content posted off duty can affect agency operations. Generally, member can reasonably be associated with the agency based on posts, language, pictures, and/or relationships with other individuals even if they themselves did not explicitly list an association with the agency.

Any form of harassment or discrimination is against agency policy.

The use of social media should not interfere with a members responsibilities. Social media use outside of work should not interfere with member responsibility or agency operations.

Members should refer to SOG on Internet Usage for determining when the use of social media is appropriate.

Nothing posted by a member should reflect negatively on the agency, other agencies, or members of either.

If a member finds themselves questioning whether something they want to post is questionable, they should generally refrain from posting the content.

Questions should be referred to the member’s Department Head.
Appendix B
ELECTRONIC MAIL (E-MAIL) AND INTERNET USAGE

Purpose:

The purpose of this policy is to establish appropriate standards and guidelines for the use of electronic mail (e-mail) and internet access within district stations and to ensure usage is consistent with district policies, all applicable laws, and the individual user’s job responsibilities.

Electronic Mail (E-mail):

E-mail is a district resource made available to members to communicate with each other, other governmental entities, companies and individuals for the benefit of the district.

A. E-mail is to be used primarily for official business purposes. Personal messages should be kept to a minimum. No solicitations should be conducted through e-mail.
B. E-mail is not a privileged communication, nor subject to privacy.
C. E-mail shall not be used to harass, torment, or disparage another party. Offensive and harassing communications are unacceptable and prohibited.
D. District users shall not intentionally seek information on, obtain copies of, or modify files, belonging to other district users, unless explicit permission to do so has been obtained.

Internet:

The district’s connection to the internet primarily exists to facilitate the official work of district members. The internet facilities and services are provided for members for the efficient exchange of information and the completion of assigned responsibilities.

A. Principles of acceptable use include the following:
   1. To respect the privacy of other users.
   2. To respect the legal protection provided to programs and data by copyrights and licenses.
   3. To protect data from unauthorized use or disclosure.
   4. To respect the integrity of computing systems.
   5. To safeguard personal accounts and passwords.
B. Unacceptable activities are those practices that do not conform to the purpose, goals, and mission of the district and to each user’s authorized job duties and responsibilities. The following list provides some examples:
   1. Private or personal, for profit activities.
   2. Use for any illegal purpose, including communications that violate any laws or regulations.
3. Transmitting threatening, obscene, or harassing messages.
4. Intentionally seeking information about, obtaining copies of or modifying files, data, or passwords belonging to other users.
5. Interfering with or disrupting network users, services, or equipment.

Monitoring:

A. This policy provides notice that there are no facilities provided by this system for sending or receiving private or confidential electronic communications. System administrators have access to all mail and user access requests, and will monitor messages, as necessary, to assure efficient performance and appropriate use. Messages or information relating to or in support of illegal activities will be reported to the appropriate authorities.
B. The district specifically reserves the right to log network use and monitor file server space utilization by users and assumes no responsibility or liability for files deleted due to violation of file server space allotments.
C. The district also reserves the right to: assign user accounts, remove a user account from the network; limit user access; revoke any system(s) access; and define, revise and/or administer any and all aspects of electronic network and communications systems.

Compliance:

A. Each district user is responsible for complying with this and all other relevant policies when using the district’s resources. Members who violate this policy may be subject to the full range of disciplinary action.
B. Questions regarding the interpretation of this policy and/or e-mail and internet usage should be directed to the member’s immediate supervisor or to the Chief and/or Assistant Chief.
Appendix C
PURPOSE
To establish procedures for proper management of Information Technology systems within the department.

Introduction
Computer Information systems (and networks) are an integral part of business at Gum Branch Volunteer Fire Department. The department has made a substantial investment in human and financial resources to create these systems.
The enclosed policies and directives have been established in order to:
A. Protect this investment.
B. Safeguard the information contained within these systems.
C. Reduce business and legal risk.
D. Protect the good name of the department.

Violations
Violations may result in disciplinary action in accordance with department policy. Failure to observe these guidelines may result in disciplinary action by the department depending upon the type and severity of the violation, whether the violation causes any liability or loss to the department, and/or the presence of any repeated violation(s).

Administration
The information management officer (IMO) is responsible for the administration of this policy. As of this time and until amended, Mr. [name removed from online version] will serve as the official IMO for the department, due to his experience in serving in this capacity with the US government.

Contents
The topics covered in this document include:
E. Statement of responsibility
F. The Internet and e-mail
G. Computer viruses
H. Spyware
I. Access codes and passwords
J. Physical security
K. Copyrights and license agreements
L. Criminal Penalties

Statement of responsibility
General responsibilities pertaining to this policy are set forth in this section. The following sections list additional specific responsibilities.
Officer responsibilities
Officers and administrators must:
1. Ensure that all appropriate personnel are aware of and comply with this policy.
2. Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all members observe this policy.
IMO responsibilities
The IMO must:
1. Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these policy directives.
2. Provide appropriate support and guidance to assist members to fulfill their responsibilities
under this directive.

The Internet and e-mail
The Internet is a very large, publicly accessible network that has millions of connected users and organizations worldwide. One popular feature of the Internet is e-mail. It is the department policy that all email that is not a department email account will not be checked while at the station. This will be done on a personal computer system outside the department.

Policy
While the department does not currently have internet access, if at a future time this should change, certain restrictions will apply as to appropriate use of department systems while online. The IMO will devise a more detailed policy at that time if needed. Until then, the following shall apply to all members:

The Internet is replete with risks and inappropriate material. To ensure that all members are responsible and productive Internet users and to protect the department's interests, the following guidelines have been established for using the Internet and e-mail.

Acceptable use
Members using the Internet are representing the department. Members are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:
1. Using Web browsers to obtain business information from commercial Web sites.
2. Accessing databases for information as needed.
3. Using departmental e-mail for business contacts.

Unacceptable use
Members must not use the Internet for purposes that are illegal, unethical, harmful to the department, or non-productive. Examples of unacceptable use are:
1. Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
2. Broadcasting e-mail, i.e., sending the same message to more than 10 recipients or more than one distribution list.
3. Conducting a personal business using department resources.
4. Transmitting any content that is offensive, harassing, or fraudulent.

Downloads
File downloads from the Internet are not permitted unless specifically authorized in writing by the IMO manager.

Department Member responsibilities
A Department member who uses the Internet or Internet e-mail shall:
1. Ensure that all communications are for professional reasons and that they do not interfere with his/her productivity.
2. Be responsible for the content of all text, audio, or images that (s)he places or sends over the Internet. All communications should have the member's name attached.
3. Not transmit copyrighted materials without permission.
4. Know and abide by all applicable department policies dealing with security and confidentiality of department records.
5. Run a virus scan on any executable file(s) received through the Internet.
6. Avoid transmission of nonpublic customer information. If the IMO is necessary to transmit nonpublic information, members are required to take steps reasonably intended to ensure that information is delivered to the proper person who is authorized to receive such information for a legitimate use.

Copyrights
Members using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by the department and/or legal action by the copyright owner.

Monitoring
All messages created, sent, or retrieved over the Internet are the property of the department and may be regarded as public information. The Gum Branch Volunteer Fire Department reserves the right to access the contents of any messages sent if the department believes, in
the IMO's sole judgment, that there is a business need to do so. All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. This means don't put anything into your e-mail messages that you wouldn't want to see on the front page of the newspaper or be required to explain in a court of law.

**Computer viruses/worms/trojans**

Computer viruses are programs designed to make unauthorized changes to programs and data. Worms are programs or algorithms that replicate themselves over a computer network and usually perform malicious actions, such as using up the computer's resources and possibly shutting the system down. A Trojan is a destructive program that masquerades as a benign application. Therefore, these things can cause destruction or overloading of department resources.

**Background**

It is important to know that:
1. Computer viruses/worms/trojans are much easier to prevent than to correct.
2. Defenses against these items include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

**IT responsibilities**

IT shall:
1. Install and maintain appropriate antivirus software on all computers.
2. Respond to all virus attacks, destroy any virus detected, and document each incident.

**Department Member responsibilities**

These directives apply to all members:
1. Department Members shall not knowingly introduce a computer virus/worm/trojan into department computers.
2. Department Members shall not load diskettes of unknown origin.
3. Incoming diskettes shall be scanned for viruses before they are read.
4. Any Department member who suspects that the workstation has been infected by a virus shall IMMEDIATELY POWER OFF the workstation and call the IMO.

**Spyware**

Spyware and adware can compromise system performance and allow sensitive information to be transmitted outside the organization. Spyware installation programs can launch even when users are performing legitimate operations, such as installing a department-approved application. As a result, combating spyware requires user vigilance as well as the IMO management and control.

**IT responsibilities**

1. Install and update appropriate anti-spyware software on all computers.
2. Respond to all reports of spyware installation, remove spyware modules, restore system functionality, and document each incident.

**Department Member responsibilities**

These directives apply to all members:
1. Department Members shall not knowingly allow spyware to install on department computers.
2. Department Members shall perform anti-spyware updates and run anti-spyware programs regularly, as directed by the IMO department.
3. Department Members shall immediately report any symptoms that suggest spyware may have been installed on their computer.

**Access codes and passwords**

The confidentiality and integrity of data stored on department computer systems must be protected by access controls to ensure that only authorized members have access. This access shall be restricted to only those capabilities that are appropriate to each department member's job duties. No persons from outside the department, except for law enforcement personnel on official business, are authorized access to the computers systems, without the IMO's consent. All other requests must be made to the IMO in writing, and the IMO (or alternate designee) must be present at the time of access.

**IT responsibilities**
The IMO shall be responsible for the administration of access controls to all department computer systems. The IMO will process adds, deletions, and changes upon receipt of a written request from the end user's supervisor.
Deletions may be processed by an oral request prior to receipt of the written request. The IMO may maintain a list of administrative access codes and passwords and keep this list in a secure area.

Department Member responsibilities

Each member:
1. Shall be responsible for all computer transactions that are made with his/her User ID and password.
2. Shall not disclose passwords to others. Passwords must be changed immediately if the IMO is suspected that they may have become known to others. Passwords should not be recorded where they may be easily obtained.
3. Will change passwords at least every 365 days or as needed.
4. Should use passwords that will not be easily guessed by others.
5. Should log out when leaving a workstation for an extended period.
6. Should not attempt to access the accounts of other users. Any violations of this rule are subject to a Level III disciplinary action.

Officer's responsibility

Officers should notify the IMO promptly whenever a member leaves the department or transfers to another department so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination.

Physical security

It is department policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

Member responsibilities

The directives below apply to all members:
1. Diskettes and portable storage devices should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up.
2. Diskettes should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
3. Critical computer equipment, e.g., file servers, must be protected by an uninterruptible power supply (UPS). Other computer equipment should be protected by a surge suppressor.
4. Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.
5. Since the IMO is responsible for all equipment installations, disconnections, modifications, and relocations, members are not to perform these activities. This does not apply to temporary moves of portable computers for which an initial connection has been set up by the IMO.
6. Members shall not take shared portable equipment such as laptop computers out of the plant without the informed consent of their department manager. Informed consent means that the manager knows what equipment is leaving, what data is on the IMO, and for what purpose the IMO will be used.
7. Members should exercise care to safeguard the valuable electronic equipment assigned to them. Members who neglect this duty may be accountable for any loss or damage that may result.

Copyrights and license agreements

It is the Gum Branch Volunteer Fire Department's policy to comply with all laws regarding intellectual property.

Legal reference

The Gum Branch Volunteer Fire Department and the IMO are legally bound to comply with the Federal Copyright Act (Title 17 of the U. S. Code) and all proprietary software license agreements. Noncompliance can expose the Gum Branch Volunteer Fire Department and the responsible member(s) to civil and/or criminal penalties.

Scope

This directive applies to all software that is owned by the Gum Branch Volunteer Fire
Department, licensed to Gum Branch Volunteer Fire Department, or developed using the Gum Branch Volunteer Fire Department resources by members.

**IT responsibilities**
The IMO will:
1. Maintain records of software licenses owned by the Gum Branch Volunteer Fire Department.
2. Periodically (at least annually) scan department computers to verify that only authorized software is installed.

**Member responsibilities**
Members shall not:
1. Install software unless authorized by the IMO. Only software that is licensed to or owned by the Gum Branch Volunteer Fire Department is to be installed on Gum Branch Volunteer Fire Department computers.
2. Copy software unless authorized by the IMO.
3. Download software unless authorized by the IMO.

**Civil penalties**
Violations of copyright law expose the department and the responsible member(s) to the following civil penalties:
1. Liability for damages suffered by the copyright owner
2. Profits that are attributable to the copying
3. Fines up to $100,000 for each illegal copy

**Criminal penalties**
Violations of Georgia law (GA Code 16-9-90/91/92/93) that are committed, are subject to the following criminal penalties:
1. Any person convicted of the crime of computer theft, computer trespass, computer invasion of privacy, or computer forgery shall be fined not more than $50,000.00 or imprisoned not more than 15 years, or both.
2. Any person convicted of computer password disclosure shall be fined not more than $5,000.00 or incarcerated for a period not to exceed one year, or both.