

## MEMORANDUM

To: Executive Director, San Francisco AIDS Foundation

From: Nikole Pagan

Date: November 1, 2005

Re: ePolicy

### Introduction

There are a number of employee related issues we need to consider as we develop and implement a computer network, intranet and email system for the San Francisco AIDS Foundation. Currently, we have no policy governing employee access to and use of the Internet, exposing SFAF to significant risk, both legal, and in terms of network security. It is therefore my recommendation that before we unveil the new technology to our staff, we must develop a policy governing its use, specifically what type of use is appropriate, what is unacceptable, and the means of enforcement. Workplace policies governing computer use and electronic communication are called ePolicies.

### Background, Analysis of Legal Requirements and Limitations & Implementation

Like many Americans, our employees probably believe that their email and Internet use is private. In general, the federal Electronic Communications Privacy Act of 1986 (ECPA) prevents employer interception of private electronic communication as it moves across a network, however, email and website information are by nature static data, and are not covered by the ECPA. Employers then have the right to monitor any Internet use or email traffic on the company system. This right is limited slightly for government employers, and government contractors, because the Supreme Court has held that public employees have constitutional rights to privacy, including First amendment speech protections, and Fourth Amendment protections against unreasonable searches and seizures. (O'Connor v. Ortega, 1987).

In US v. Simmons (2000), the 4<sup>th</sup> Circuit Court of Appeals held that public employees do not have a reasonable expectation of privacy of electronic communication where the employer had a policy specifically

outlining what types of data and use would be monitored, and how that information would be controlled, accessed and audited, with clear penalties for violation the policy. Accordingly, a well-written ePolicy that is effectively communicated to our staff is our best protection against the many risks associated with employee computer use, and access to the Internet (Flynn, 2001).

There are issues of SFAF's liability concerning employee conduct such as sexual harassment & discrimination, criminal activity such as terrorism, and intellectual property theft such as software piracy. There are network security issues: websites and email attachments containing viruses and Trojan horses could cripple or disable our network, as could attacks by remote computer hackers. If we choose to monitor employee use of the Internet and email there are employee privacy issues, and legal compliance issues should logs of such monitoring be requested as Discovery in any litigation. (Lasprogata, et al., 2004). There are productivity issues: studies have shown as much as 40% of employee Internet use is not work-related (Business Wire, 2001).

We have not noticed a significant productivity drop-off in our organization due to Internet access. There is no reason to assume use of an Intranet or company provided email account would suddenly create a huge productivity loss. In fact, there is some merit in allowing employees personal use of the Internet and their email accounts for activities such as banking, bill-paying, making appointments, communicating with children via email, booking travel arrangements; activities that in the past might require time away from the office, now can be accomplished with a few quick keystrokes and clicks of the mouse. By allowing some personal use, as long as it complies with the written ePolicy, we show our employees that we are concerned for their quality of life, and trust them enough to make informed decisions about what personal use is acceptable. This will be key in their acceptance of the new policy.

Absent an ePolicy, I believe it is the other risk factors listed in the preceding paragraphs that could prove most costly, both financially and in terms of human resources. One employee illegally downloading a copyrighted piece of software, for example, could result in a federal fine of \$150,000. (Flynn, 2001).

We must also consider our duty to create a harassment and discrimination free workplace. Our ePolicy must address the use of the Internet or SFAF's email to obtain or distribute information that is harassing, sexually, explicit, discriminatory, defamatory, or otherwise creates a hostile work environment. Organizations have been accomplishing this via the use of software that monitors emails and flags key words, monitors website visits, or prohibits access to pornographic websites.

As an HIV/AIDS service-based organization, there are legitimate reasons our staff may need to send emails or visit websites with sexually explicit content. Blocking access to such content is not fitting with SFAF's goals. Our policy then, should address harassment, and prohibit access to sites with illegal pornographic content, such as child pornography.

We need to monitor the use of the technology, but to what extent, and what kind of records should we keep? The very nature of a computer network enables users to store huge amounts of data, far more, and for longer, than with paper records. Keeping extensive logs of employee Internet use is possible through the use of software. It is possible to back up all saved emails when we back up the network each night. Emails can remain in an employees account indefinitely. Any records kept are subject to subpoena or discovery request. Should we need to produce backed-up email and web log documents as part of a workplace lawsuit, or as compliance with a Patriot Act terrorist investigation, we could be looking at tens of thousands of dollars to produce even a single day's back-up. (Flynn, 2001).

As we roll out the policy and begin training our staff in compliance, we must encourage deletion of unnecessary email messages. Staff must be advised not to automatically save any email, and instructed how to access and delete files from their account's "manual delete folder", commonly known as "Trash". This has proven to be a difficult area for other organizations as they implement ePolicies. Many people are not aware that a simple "delete" of an email sends the message to the "Trash" folder, which can store email indefinitely, unless programmed to delete on a regular basis. Our ePolicy must address both the need to

delete unnecessary email, and the length of time any deleted email will be stored. Some organizations store up to 30 days of email prior to deletion, and some program their Trash folders to empty daily.

Our agency's culture has long fostered an atmosphere of respect, dignity, and personal responsibility amongst our staff, at all levels. Suddenly implementing an ePolicy that seems very restrictive, places limits on privacy, and smacks of Big Brother watching them, regardless of legality, will likely alienate and anger a sizeable portion of our staff. Because personal privacy is such a sensitive issue, it would be wise for us to assume that our staff as a whole will have objections to this policy. Sensitivity to their concerns is going to be a key element in implementation. (Lane, 2003) We can address these concerns via education and training, and management outreach.

Before we rollout the new policy to the rest of the staff, we need to educate and train our managers, and get them on-board with the implementation of the new policy. Our managers should be our first line of defense. It will be to the managers that employees turn for guidance, with questions, and to air their grievances. The better prepared managers are to handle these issues with accuracy and concern, the less likely we are to experience a decline in morale based on our employees' perceived loss of privacy, and narrowing of their rights.

By scheduling multiple training sessions, and continuing education, we demonstrate an ongoing commitment to making sure our employees are informed about our ePolicy and are in compliance. By giving our employees a clear idea as to the rights they retain, and linking the continued success of SFAF as an efficable AIDS services organization to employee compliance with the policy, we instill in them an idea of ownership of the policy: they are responsible for their actions, which in turn, are responsible for the ability of SFAF to reach our organizational goals.

## **Conclusion**

As the unveiling of our SFAF's intranet, network, and email systems approaches, it is imperative we address the various legal issues associated with employee use of such technology. A comprehensive

ePolicy that covers appropriate use and employee misconduct will substantially reduce SFAF's liability. A program of training, ongoing education and management outreach is key to employee acceptance of any policy during its implementation, but even more so when privacy rights are at issue. An effective ePolicy will attend to all of these issues, limit SFAF's liability, and inform employees of their rights, expectations, duties, as well as lay out the consequences of violation.

### **Suggested Policy Language**

San Francisco AIDS Foundation provides a computer with Internet and Intranet access and an electronic mail account to each employee as a means to facilitate enhanced internal communications, better customer service and reduction in retention of unnecessary paperwork.

These guidelines govern your use of SFAF's electronic equipment.

1. Users shall not harass, threaten, intimidate others, or engage in illegal activity, including accessing, collecting, or distributing electronic information (including child pornography, terrorism, espionage, theft or drugs) by email or other postings. All known violations should be reported to management for appropriate action.
2. Users may not use SFAF's email, network, or Internet/Intranet access for offensive or harassing statements or language, including disparagement of others based on their race, color, national origin, religion, disability, age, sex or sexual orientation.
3. Users should not automatically save all email communication. Any email stored in the "Manual Delete" or "Trash" folder will be automatically deleted after 30 days.
4. SFAF monitors all websites visited. It is specifically prohibited for employees to knowingly visit websites featuring child pornography, terrorism, espionage, theft or drugs.
5. Users may not copy any software, applications or programs installed on SFAF's computers for use on personal computers or laptops, or for any other reason, without authorization. Users may not import, download or store copyrighted materials on any SFAF computer without permission from the author. Doing so may violate application license agreements and/or copyright law.

Your use of the Network, Intranet, Internet and SFAF-provided email account is a privilege, and not a right. If you violate the provisions of this policy, at a minimum access to the Network, Intranet, Internet and email account may be suspended or revoked.

## REFERENCES

- Electronic Communications Privacy Act of 1986. 100 STAT. 1848 PUBLIC LAW 99-508--OCT. 21, 1986
- O'Connor v. Ortega, 480 U.S. 709, 715 (1987)
- U.S. v. Simmons, 206 F.3d, 398 (4<sup>th</sup> Cir. 2000)
- Lasprogata, Gail, Nancy J. King, Sukana Pillay. "Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada." Stanford Technology Law Review, Stanford, 2004. Retrieved October 15, 2005 from [http://stlr.stanford.edu/STLR/Articles/04\\_STLR\\_4](http://stlr.stanford.edu/STLR/Articles/04_STLR_4)
- Business Wire. "Employee Internet Misuse a \$63 Billion Problem For Corporate America, Reports Websens Inc.; Misuse May Affect U.S. Productivity Overall, Which Recently Hit Eight-Year Low:". Business Wire, San Diego, August 1, 2001. Retrieved October 17, 2005 from <http://www.highbeam.com/library/docfree.asp?DOCID=1G1:76892431&ctrlInfo=Round18%3AMode18c%3ADocG%3AResult&ao>
- Lane, Frederick. *The Naked Employee: How Technology Is Compromising Workplace Privacy*. New York: AMACOM, a division of American Management Association, 2003.
- Flynn, Nancy. *Designing and Implementing Effective E-Mail, Internet, and Software Policies*. New York: AMACOM, a division of American Management Association, 2001.
- Findlaw's Modern Practice. "The Weblog Chronicle - DOOCES WILD: How Employers Can Survive the New Technological Poker Game of Employee Blogging." By Philip L. Gordon and Christopher E. Cobey of Littler Mendelson, October 2005. Retrieved on October 19, 2005 from <http://practice.findlaw.com/blogger-1005.html>
- Loeb & Loeb, LLP. "Minimizing Employer Liability for Employee Internet Use" Carla J. Feldman and Michael P. Zweig. New York: Loeb & Loeb, LLP, September 2000. Retrieved October 16, 2005 from <http://www.loeb.com/CM/Alerts/alerts126.asp>