



# Web Policy Management

*An Individual Employee's Perspective*

**Wavecrest Computing**  
2006 Vernon Place  
Melbourne, FL 32901  
Toll-free: 877-442-9346  
Voice: 321-953-5351  
Fax: 321-953-5350

**[www.wavecrest.net](http://www.wavecrest.net)**

*(1) Policies must be clear, specific, and understandable; (2) management needs to become more educated and involved in the process, and; (3) employees need to be educated, early on, on all aspects of the Web policy and its relationship to the success of the enterprise.*

## Preface

This paper discusses several aspects of Internet management policy. It was written by an employee of a typical corporate organization that, like so many others, uses the Internet in the conduct of its business. The purpose of the paper is to stress the need for clear, viable Internet management policies in large organizations.

The paper has three main sections. The first discusses the Web-use policy used by the author's organization. In particular, it highlights the shortcomings of that policy as perceived by the author. The second part of the paper describes how that policy was applied to several "Web abuse" situations in a less than ideal manner. The third section provides some recommended solutions to the overall Web policy management challenge.

Despite the fact that the paper was written by a non-management person, it clearly underscores the complexity of the overall Web policy management challenge. Equally important, it brings out three pressing needs in the world of Internet usage and Internet policy management. That is, (1) policies must be clear, specific, and understandable in the first place, (2) management needs to become more educated and involved in the process, and (3) employees need to be educated, early on, on all aspects of the Web policy and its relationship to the success of the enterprise.

For obvious reasons, the author requested to remain anonymous and asked that we not disclose the exact name of the corporation discussed herein. We are, of course, honoring these requests, and we do not believe that anonymity dilutes the strength of the messages contained herein.

## Introduction

Most modern businesses rely on computers as necessary tools for their employees. In recent years it has become commonplace for companies to provide their employees with Internet and email capabilities for their office computer systems. These features are versatile and useful time-savers for the average employee, but they can also create problems for both the companies and the individual workers. Management's monitoring of employees' computer systems has become possible, and in some cases necessary. The amount and content of email messages that people send and receive can be checked from behind the scenes, as can the types of Web sites that employees visit while using the Internet. Companies can purchase computer programs that will check to see what the employees are doing while they are logged on to the office network system.

My company uses these types of programs to identify employees who are abusing the computers that have been assigned to them. The computers legally belong to the U.S. Government, as our corporation is in a contractual business arrangement with a Federal agency. When we log on to our computers, the first thing that comes up on our screens is a warning. It is a brief statement informing us that our computers and our interoffice network are subject to monitoring, and that our computers are to be used only for business-related purposes.

About a year ago, the department in which I work was subjected to a sudden increase in employee terminations, disciplinary actions and letters of caution. Word soon got out that the employees who had been fired or disciplined had all been "abusing the email and/or the Internet." Rumors and gossip around the office went out of control. No one knew for sure what the employees had done, only that some were fired and some were given time off without pay. Still others were given letters of caution in their personnel files.

*The guidelines for what constitutes "abuse" need to be made clearer and defined better.*

Certainly, my fellow employees should know better than to use their assigned computers for personal business. However, when we first got email capability, people typically responded by sending the occasional joke, funny picture, or invitation to a luncheon or retirement party. These little morale boosters brightened up the workday and seemed harmless enough. Email was still used primarily for business contacts. I never clicked my Internet icon at work, mainly because my job does not require that I do any online research. If I surfed the Web, it would have been for my personal enjoyment, and that was something I should do at home. When at work, I am supposed to be working.

As it turned out, some of the employees that were disciplined had been sending excessive emails, some as many as thirty personal messages per day. Some messages contained obscene language and graphic photo attachments. They were receiving these messages and then forwarding them to other employees. These workers deserved to be disciplined, but to what degree? What should the punishment be for sending a joke vs. the punishment for sending nude photographs? One lady, known to be religious and conservative, was given a letter of caution for sending out a flyer for a church group meeting. Obviously, the guidelines for what constitutes "abuse" need to be made clearer and defined better. At the time of this incident, Internet abuse was a new problem, and real solutions had not yet been developed.

While management was supposedly reviewing old backup tapes, looking at emails sent months earlier, the employees went into a panic. Would we be the next ones fired? Most of us, including my direct supervisor, had been guilty of sending jokes, party flyers, and school-related materials to our college professors. Would we be swept up with the people downloading pornography and sending obscene photos to their friends?

In my view, the company handled the situation very poorly. Management never made it clear to the workforce specifically what the punished employees had been guilty of. They never differentiated between the various offenses, as to why some were terminated and others were not. Even worse, it appeared that employees might have been fired based on their position in the company. One female clerk had her computer abruptly confiscated, and was fired within two days. Her offense was excessive personal emails, the same offense as a male engineer. His punishment was one week off without pay. Some employees received "final letters of caution" when they had never received a "first" or "second" letter of caution. Still others, including myself, received no punishment whatsoever. This is not fair or equitable, considering that I had emailed some jokes and personal letters in the past.

Is any or all of this unfair? Maybe the woman who was fired lied about what she had done and had actually done something far worse. This is possible, but the employees who remain on staff need to have clear guidelines to go by. Instead, the whole matter was dropped. It disappeared just as quickly as it had arrived. We no longer heard about anyone being monitored online or disciplined for email abuse. Did management stop checking, or did they decide they had better back off because they had created such unrest in the work environment?

Most employees frantically deleted all personal files and refrained entirely from using their computers for anything that was not business related. Of course, this was the result that management wanted, but it was extremely bad for company morale. Paranoia and gossip ran rampant, creating a working atmosphere that was distracting, unhappy, and negative. I was afraid to invite a co-worker to lunch via email! In terms of efficiency, our department suffered due to the time people spent whispering, wondering, and worrying.

The company that I work for is large and diverse, with many separate departments.

It was only in my department where this email/Internet scandal took place. Consequently, I continued to receive humorous personal emails and jokes from employees in other departments. They were stunned to hear that they could get us fired for sending what they referred to as "morale mail." My departmental co-workers and I called them on the phone and told them never to send us email messages unless they were work-related. Why were some organizations within the company treated differently from others?

My employer and other companies like it face difficult decisions when it comes to tackling the problem of employee Internet/email abuse. How far can management really go toward

*My employer and other companies like ours, face difficult decisions when it comes to tackling the problem of employee Internet/Email abuse. A fair solution must be reached which addresses the problem from the perspectives of both the company and the individual employee.*

*Management must proceed in a thoughtful and deliberate manner.*

preventing inappropriate use of the Government owned computers? There would never be enough time or manpower to monitor every employee and follow up on every suspicious transaction. Such monitoring opens the door to other questions as well. For example, the phones that we use are Government owned also. I have never heard of anyone being fired for calling co-workers to verbally tell a joke, or to invite someone out for lunch. As a matter of fact, it might be more time-efficient to email a friend than to walk to their desk and chat, or to linger by the water-cooler for office gossip and sports roundups. Email can conceivably fall into the category of a "work-break." Some people go out for a smoke or a soda, others like to write a quick note to their friends.

A fair solution must be reached which addresses the problem from the perspectives of both the company and the individual employee.

### **A Possible Suggestion**

In my view, the first step toward resolution should be to form a problem-solving team for this issue. The team should be comprised of men and women, with someone to represent each department of our company. The team members should not all be members of management. As a group, they should begin to develop solutions, including a detailed policy and procedure. This should be more than a vague disclaimer in tiny print on our computer screens. It should be a hard-copy document given to each employee, requiring their signature as proof that they understand it and will comply. It should be a detailed list of exactly what constitutes wrongdoing and why, and exactly what will happen to them if they do not abide by the rules. The procedure should be reviewed and updated at least every year, and it should be distributed to all employees of the company.

Another option to consider would be removal of Internet and email capabilities from the computer systems of each individual employee. This way, those who truly use these features in their daily jobs could be identified and permitted to use shared, centrally located systems set up for the sole purpose of Internet research and email communications. Certainly, some engineers use the Internet and email to contact vendors, order parts, register for training seminars, etc. But other employees, such as myself, do not need the Internet to perform their jobs, and could go to the shared systems if we occasionally needed to. The shared systems could be set up with log-in passwords, so that management could see exactly who used email or the Internet at what time, how long they spent, and what Web sites they visited. Is drastic reduction in access the best or only way to handle this aspect of a difficult problem? Probably not, and this is just one small suggestion, offered for consideration. More and better ideas are needed.

Management must proceed in a thoughtful and deliberate manner. To turn back the clock on the technological advances that we have made places our company's employees, and the company itself, at a disadvantage in the business world. On the other hand, what problems and disadvantages do members of management face when some of their workers abuse the trust that the U.S. Government has placed in our company? These issues must be addressed too. As I see it, the overall situation is a case of "one bad apple spoils the whole bunch," and equitable solutions don't come easy. The majority of employees can be trusted to perform their jobs to the best of their ability and to utilize the tools of their trade without abusing them. Should we all be punished because a few of us use poor judgment and show a blatant lack of respect for our customer who actually owns and pays for the resources we use?

Until solutions are found, and something official is in place, the wrongful abuse of Government computers, as well as the unfair treatment of certain employees, will most likely continue.