



## Internet Monitoring in the Workplace: A People Issue

**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)**

## Abstract

This paper is written for mid to large-scale organizations—businesses, schools and government agencies—that grant Web-access to their workers or students. Its focus is policy-based Web-use management, i.e., the process of ensuring that institutional computer users access the Web for productive, work-related purposes only. It asserts the following:

- Although technology is involved, employee Web-use management is primarily a *people* issue, not an IT or IT-security issue.
- Because it is fundamentally a people issue, HR personnel should either take the lead or work closely with IT in proposing and developing solutions.
- Employee Web-use management is a way for HR to contribute to the productivity and profitability of the organization.

The paper first discusses casual surfing in the workplace, i.e., employees visiting Web sites for non-work related purposes. The author points out how such activity can degrade workforce productivity, impact network performance, and create legal liabilities. Needless to say, any and all of these outcomes can seriously degrade the organization's bottom line. Effective employee Web-use management programs are essential to prevent this from happening, but they need to be implemented without destroying workforce morale.

Because this subject deals with human behavior in the workplace, the paper discusses why HR personnel are the professionals best equipped to take the lead in developing and implementing employee Web-use management efforts, collaborating as required with executive management, functional managers and IT personnel.

The paper then examines the main elements of an effective employee Web-use management program, i.e., Web-access policy, training, and compliance. Implications for workforce morale are also explored.

Also discussed is the availability of HRIS (human resources information systems) tools that can help in the effort. In particular, Web-access filtering and reporting software can be key elements in the overall solution. However, as the author points out, they need to be chosen carefully to ensure accuracy, effectiveness and flexibility.

The author concludes on the following note: Although effort is required, the employee Web-use problem *can* be successfully managed with proper HR and management attention — much to the benefit of the organization.

## I. Introduction

**General.** Employee Web-use management was unheard of a decade or so ago. The need has emerged in most workplaces during the last ten or twelve years because of the tremendous expansion in the use of desktop computers with Internet and intranet connections. This phenomenon gives millions of workers access to millions of Web sites. Such access can be a real boon to businesses and other organizations, or it can be a serious problem — as discussed in Section II, Background and Section III, Web-use Management Programs. First though, let's look at the subject from a conceptual perspective, i.e., just what kind of an issue is it?

*HR personnel are the professionals best equipped to take the lead in developing and implementing employee Web-use management efforts.*

*Web-use management is fundamentally a people issue, one that involves human behavior in the workplace.*

**It's a People Issue.** Because of its relationship to computers and networks, many people mistakenly believe that Web-use management is primarily an IT issue, one that can somehow be solved with user IDs, passwords, firewalls and the like. This is simply not the case. *Web-use management is fundamentally a people issue*, one that involves human behavior in the workplace. Computers don't visit Web sites. People do. Employees can choose to visit certain Web sites for productive, work-related purposes, *or they can choose to visit other sites for nonproductive, personal purposes*. They may or may not do the latter innocently, and for that matter, they may or may not even *know* what types of visits are appropriate or inappropriate in their particular workplaces. In addition, they may or may not work in an atmosphere that fosters inappropriate use of Web-access resources. And finally, they may or may not have a clear-cut Web usage policy to guide their online behavior.

**HR Involvement.** For all of these people-oriented reasons, there is a clear need for HR personnel to take the lead — or at least be seriously involved — in developing and implementing effective employee Web-use management programs.

That is the focus of the remainder of this paper.

The next section presents some background on the problem. Subsequent sections discuss (a) who should be responsible for resolving the problem and (b) what kinds of efforts are required to do so.

## II. Background

The explosion in use of personal computers with Web access is truly a good news — bad news phenomenon.

**The Good News.** From a business or mission perspective, there are many valid reasons for workers to access Web sites, e.g., to perform important business processes and research tasks, procure materials and supplies, etc. Such access can and does contribute much to the agility, efficiency, innovativeness and success of the enterprise. And it is becoming more and more integral to the performance of core business functions every day.

**The Bad News.** On the other hand, Web-access has significant *negative* potential. Because the World Wide Web is so interesting, wide ranging, and information rich, employees can — and often do — waste considerable working time and network resources accessing various sites for personal reasons. Wasted time obviously represents reductions in productivity and efficiency and thus unnecessary cost. Note the following:

- 30 to 40% of Internet use in the workplace is not related to business. (IDC Research)
- 37% of workers say they surf the Web constantly at work (Vault.com).

**Legal Liability Exposure.** Unfortunately, one of the most serious forms of Web-access abuse — and thus waste — involves the downloading and display of pornography. Such activity not only detracts from work force productivity, it can lead to legal liabilities, primarily in the form of sexual harassment and hostile workplace lawsuits. Typically, such suits are filed by employees who have inadvertently or deliberately been exposed to pornographic images downloaded by other employees. Here are a few of the myriad statistics on the subject:

- According to SexTracker, porn sites receive more than 27 million hits per day, with top sites receiving a staggering 2.8 million hits per day.
- 70 percent of all Internet porn traffic occurs during the 9-to-5 workday, according to SexTracker. This means that one in five workers access cybersex at work.
- Pornography on the Internet generated \$1 billion in revenues in 1998 and represents 10 percent of total e-commerce business, according to The Industry Standard.

From the Department of Labor...The US Department of Labor estimates that wasted time costs corporations up to \$3 million a year for every 1,000 employees, as reported in *TheStandard.com* (January 2000). The article continues: "Where are employees wasting most of their time these days? It's not the water cooler. Companies that want to improve efficiency are looking to rein in web-surfing workers..."

**More Bad News.** Workers can also waste time on legitimate but *unproductive* visits. Such waste can stem from flawed business strategy, poorly designed processes, faulty managerial decisions, or misguided supervisory direction. Such misuse can represent missed profit opportunities and degrade ROI on the organization's investment in information technology.

**The Solution.** Managing employees' use of Web-access resources is a sensitive and complex task, one that deals with policy, training and compliance issues, and one that's crucial to productivity, profitability and morale in the workplace. Serious and informed managerial leadership is required, as is a well-organized and multi-faceted program.

These subjects are explored in the following sections, with emphasis on the need for HR involvement and leadership.

"Companies that do not monitor employees' surfing habits make themselves vulnerable to legal liabilities, probable bandwidth abuse and employee productivity gaps." — *The Aberdeen Group*

### III. Responsibility for Employee Web-use Management

**General.** As discussed above, every organization that provides Web-access to its computer users needs an effective Web-use management program. Although some may not concur, let's assume there is agreement on that point.

This being the case, the question immediately arises: "Who should be responsible for developing, implementing and managing the program?" In this case, a corollary question might be: "Isn't Web-use management an IT or IT-security issue?" Let's explore these questions, beginning with the latter.

#### 1. Web-use Management vs. the Role of IT

As mentioned earlier, many people think (or *like* to think) that Web-use management is solely an IT issue, one that can and should be solved by IT personnel. But, as also pointed out earlier, the fundamental problem is a *people* (workforce) issue, one which IT personnel typically are not suited for by virtue of training, experience, resources and long-standing traditional responsibilities. Let's look at IT's typical charter and capabilities:

- IT is responsible for providing the best possible infrastructure and applications, but they're not responsible for how these resources are used functionally on a day-to-day basis. Example: IT can give you Microsoft Word, but they can't control what you write.
- IT is responsible for solving technical problems. Web-use management is not a technical problem; it's a people problem.
- IT personnel can certainly institute a simple pornography-blocking process, but they're not equipped or trained to deal with the larger issues of lost productivity, employee behavior, workforce morale, disciplinary actions, potential litigation, etc. And to attempt to have them do so would constitute a huge waste of technical talent.
- So while it's pretty obvious that IT can provide some technology to help out, they are *not* in a position—nor *should* they be—to design, implement, and manage an *overall* employee Web-use management program.

#### 2. Employee Web-use Management: a Team Effort, Led by HR

An effective employee Web-use management program will involve multiple areas of the organization. Consequently and ideally, employee Web-use management should be a team effort involving five elements:

- **Human Resources (HR) Personnel.** HR is best equipped to take the lead, initiate policy, suggest tools and processes, orient and train employees, etc.
- **Senior Management** (CEO, senior division managers, etc.). Senior management needs to provide overall guidance, approve policy and processes, establish corporate culture, support HR and IT efforts, stay involved, etc.

On average, non-work related surfing costs American businesses \$54 billion and 30%-40% in productivity losses every year.

- **Information Technology (IT) Personnel.** IT personnel can help evaluate, select, install, and set up software tools.
- **Department Managers and Supervisors.** Managers and supervisors need to use reports, counsel employees, recommend blocking regimes, stay involved, follow up, etc.
- **Individual Users** (e.g., employees). Individual users should know the policy and use Internet and intranet Web access properly and not for personal purposes.

While all five of these are important, leadership by HR is particularly critical. It's explored further in the next section.

#### IV. Leadership by Human Resources

**General.** As indicated above, Web-use management is all about employee behavior, productivity and morale, and its resolution involves matters of policy, training and compliance. Because HR organizations are accustomed to dealing with similar or related matters, they are in the best position to take the lead in instituting effective employee Web-use management programs. (HR organizations typically contain experts in personnel policy, codes of conduct, labor relations, workforce training, legal compliance issues and workforce morale, all of which relate to the employee Web-use management issue.) In addition, by virtue of their personal backgrounds, orientation and job responsibilities, HR personnel are in the best position to be objective in this sensitive area. Objectivity and even-handedness are necessary to strike an optimum balance between overly rigid controls on the one hand and total laxity on the other. In sum, by taking the lead on this issue, HR personnel can:

- Make a positive contribution to workforce productivity and organizational profitability.
- Help keep the company out of severe legal difficulty.
- Help maintain/improve workforce morale.
- Ensure a balanced approach to Web-use management.

"On average, non-work related surfing costs American businesses \$54 billion and 30%-40% in productivity losses every year. Businesses lose an estimated 26 million manhours annually to online game playing alone." — *The Gartner Group*

**HR's Specific Role.** If HR personnel accept this challenge, they will need to do a number of specific things to ensure successful and effective employee Web-use management. For example they will need to:

- Educate senior management on the importance of employee Web-use management, get their inputs, and keep them involved.
- Establish a sound Acceptable Use Policy (AUP)—consistent with company culture. Communicate the policy to the workforce.
- Establish Web-use training programs for managers and employees.
- Work with functional managers and IT to ensure optimum implementation.
- Revise Web-use policies when experience dictates.
- Stay abreast of related legislation and litigation.
- Follow up, stay involved. Work with functional managers on specific cases.
- Utilize reporting and blocking tools that are reliable and accurate.

Informed and motivated HR professionals can do these things well — in the framework of a well-designed Web-use management program. The next section describes the elements of such a program, one that can go a long way toward ensuring optimum use of Web access in the workplace.

#### V. Employee Web-use Management Programs

**General.** The previous sections pointed out *why* an effective employee Web-use management program is essential to today's businesses and who should be responsible for leading its

*A crucial and prerequisite component of an effective Web-use management program is a carefully crafted Acceptable Use Policy (AUP).*

design and implementation. This section provides a summarized analysis of such a program. The analysis recognizes that the specifics will vary from case to case in accordance with the business or organization's culture and management style.

**Definition.** Employee Web-use management is the continuous process of ensuring that workers use Web access for productive, work-related purposes only. At a conceptual level, it can be likened to other areas of personnel management such as:

- Controlling personal telephone calls in the workplace.
- Controlling and preventing employee theft of company property.
- Policies to maximize productivity, e.g., limits on lunch & other breaks.
- Controlling use of company property for personal use, e.g., vehicles, copiers, etc.
- Labor distribution and cost Accounting, to track how resources are being used.
- Use of employees' code of conduct (ethics and integrity in the workplace).

"Porn sites are the diversion of choice, but shopping, day-trading, and Net affairs also help while away nearly a third of the average workday." — *Business Week*, June 12, 2000

**Requirements of an Effective Program.** To be effective, employee Web-use management requires that responsible HR personnel and other management personnel do five things:

- Develop a sound Acceptable Use Policy (AUP)—consistent with corporate culture.
- Communicate that policy clearly to all computer users (tell them what's acceptable and what's not, etc.).
- Train employees on how to use Web-access productively.
- Use reliable software tools that are designed specifically to (a) monitor compliance with Web-use policy and (b) proactively control Web access.
- Follow up with corrective actions when inappropriate access is detected.

If they do these things well, misuse and abuse of network resources will be minimized without damaging workforce morale. These six elements are discussed below.

**1. The Acceptable Use Policy (AUP).** As mentioned above, a crucial and prerequisite component of an effective Web-use management program is a carefully crafted Acceptable Use Policy (AUP). Fundamentally, the AUP spells out in writing what type of Web-access activity is acceptable, what type is not, and the consequences of engaging in the latter. An effective AUP will be clear, detailed, unambiguous and reflective of the corporate culture.

Most importantly, the AUP should include ground rules and standards for what constitutes "desirable", "acceptable", "unacceptable" and "abusive" use of the Internet and other network resources. In other words, the policy and rules must address the question: "For our *particular* organization and, for that matter, for specific departments and individuals *within* the enterprise, exactly what constitutes legitimate productive use of the Internet, and what constitutes *abuse*?"

Depending on the corporate culture, some activity may be defined as "acceptable" usage even if such usage is not strictly for business purposes. For example, a few minutes to check the stock market or sports scores during lunch hour may be perfectly acceptable and may be conducive to good morale, but exceeding the "limit" may be abusive. This provision enables the enterprise to permit (yet control) limited use of network resources for personal/morale reasons.

The policy should also state clearly how compliance will be monitored and what the consequences to the individual of abusive use of network resources will be. In sum, the policy needs to be carefully crafted, well-defined, precise *and reasonable*. It must also be specific to the enterprise, easily auditable, and clearly communicated to all concerned in easily understood language.

*Having published a sound AUP and trained the workforce in proper use of network resources, management now needs to monitor and control Web usage.*

There are several reasons why well-designed AUPs are so important:

- People work best when they know the rules.
- Rules serve as the baseline for gauging acceptability.
- Rules can be built into monitoring and control tools (category ratings, abuse thresholds, access denials, etc.)
- Reasonable rules encourage appropriate behavior and discourage inappropriate behavior.
- Clear policies minimize (if not eliminate) the necessity of management intervention.
- Workers will be demoralized by enforcement of unstated or unclear policies.

**2. Communicating the Policy to All Concerned.** The policy should be provided in writing to all concerned. This includes management personnel as well as the general workforce. All recipients should be required to sign and return a copy of the policy to HR, indicating that they have read and understand its contents. HR and management personnel should hold meetings with workgroups to answer questions and provide additional information.

**3. Training the Workforce on Use of Network Resources.** In addition to communicating the policy to all concerned, HR and management personnel should conduct broader-based training sessions covering Web usage and related subjects. The purpose should be to encourage proper and productive use of network resources while reinforcing the information in the AUP.

**4. Employee Privacy and Workforce Morale Issues.** Some people might view employee Web-use management as a violation of privacy. However, courts have ruled consistently that employers have a right to ensure that their property and resources are not being stolen or used improperly by employees. Competent management can prevent damage to morale by employing enlightened, open, progressive approaches. This includes implementation of a reasonable and rational policy, clear and honest communications, and reliable metrics.

**5. Use of Software Tools.** Having published a sound AUP and trained the workforce in proper use of network resources, management now needs to monitor and control actual usage. Software tools can help this part of the program. Basically, software can do two things:

Monitor Web Usage. Software is available to monitor compliance and ensure conformity with the organization's AUP. The software should be configured to do its job in a constructive and reasonable manner. Such monitoring can and should identify positive, desirable Web usage as well as negative trends and unacceptable use. By keeping track of employees' efforts in this way, effective leaders will get to know their people better, give better directions, and motivate their workforce. They will also be able to keep projects on track, boost productivity, and correct mistakes before they turn into serious problems.

Block Access to Specified Web Sites. Software is also available to selectively block users' access to designated Web sites while allowing access to other sites. Sites that can be blocked are those in "totally unacceptable" categories such as those related to pornography, illicit drugs, "hate" discussions, etc. Also sometimes included are categories that *might* be considered inappropriate, e.g., gambling, games, sports, shopping, finance, chat, etc.

With respect to the selection of tools, management should insist on software that:

- Was developed from the ground up for managing *human* behavior, not tracking "bits and bytes." What's needed is an HR tool, not an IT or IT-security tool.
- Was developed solely for outbound reporting and control and is not an adaptation of a tool developed for inbound reporting.
- Differentiates true "visits" (clicks initiated by human action) from extraneous or irrelevant hits.
- Counts clicks to measure the extent of activity and doesn't claim to measure time on site; it can't be done.
- Uses a broad-based list that doesn't just focus on legal liability sites.

- Was developed by a firm that specializes in Web-use management across the board, not just prevention of legal liability.
- Is furnished by a vendor that provides complete and effective follow-on support. Provides information that is actionable, reliable and accurate.

With respect to the last item in the above list, high levels of accuracy and reliability are essential to ensure that:

- Employees are not falsely accused of Web-access abuse.
- Managers reach sound, valid conclusions when assessing Web use activity.
- Managers make well-founded decisions and take appropriate corrective action.
- Different managers and departments make consistent interpretation of results.
- Policy enforcement is consistent from department to department.
- Management stays on solid ground legally.
- The workforce's morale is not damaged.

**6. Management Follow-up Action.** With a policy in place, with personnel oriented, with the workforce trained, and with software busily monitoring and controlling Web usage, there's nothing left to do, right? Wrong! The software will inevitably reveal patterns of inappropriate usage or disclose signs of outright abuse. These will all require attention by HR and/or management personnel.

With good tools, management can identify about 80 percent of the visited sites. They can also use software to block access to about the same percentage of inappropriate sites. Suspected problem areas in the unidentified 20 percent can be followed up on an individual case basis (using customized audit reports).

After identifying the problems, management can take appropriate follow-up actions such as counseling employees, training or retraining workers, changing work processes, and revising or clarifying the AUP. Managers may also need to institute follow-up audits on individual users and, in worst cases, take disciplinary action including termination.

## VI. Summary

*Employee Web-use management is a people issue, not solely an IT challenge.* It deals exclusively with human behavior in the workplace. It's a complex, never-ending management challenge, with serious implications for the business's bottom line. And it must be pursued constantly, in a firm but fair manner.

By virtue of training, experience, temperament and mission, HR personnel are the best equipped to take the lead in implementing firm but fair employee Web-use management programs.

The objective of such programs should be to capitalize on the beneficial, productive potential of Web access while precluding or minimizing its negative aspects. The challenge is to achieve this objective in a *balanced* way, *one that fosters and promotes the interest of the enterprise as a whole without creating an oppressive "Big Brother is watching you" climate in the work place.* This is a delicate balancing act, one that is not easy to define and achieve. Recognition of the following will help:

- *It's all about people and their behavior.*
- Inappropriate and improper use of Web-access in the workplace is a critical and potentially costly issue.
- The biggest Web-use problems stem from human nature and the size and rapid growth of the Web.
- Web-use management is not primarily a technical or IT issue, and it can't be solved with technology alone (although IT personnel and technology tools can certainly help).
- Highly accurate tools are essential to success of the program. Such tools are designed *from the ground up* for monitoring human activity, not for tracking bits and bytes.

*The objective of successful Web-use management programs should be to capitalize on the beneficial, productive potential of Web access while precluding or minimizing its negative aspects.*

- With good tools, management can identify about 80 percent of Web-use activity and block access to about the same percentage of inappropriate sites.
- Suspected problem areas in the other 20 percent can be followed up on an individual case basis (using customized audit reports).
- Employee Web-use management deals with issues of *policy, training, and compliance*, and good communications are critical to all three.
- HR personnel are best equipped to take the lead in Web-use management efforts.

Admittedly, effective Web-use management is a real challenge, and there will be hurdles along the way. But then, worthwhile objectives are never easy to achieve, and stubborn obstacles *can* be overcome. The payoff can be big.