Internet Acceptable Usage Policy Guidelines

OVERVIEW

Why Should You Care About Internet Usage?

1. Employee Productivity: Organizations typically measure productivity based on specified goals and objectives, as well as by examining how employees allocate their time. Management should have the information they need to examine how employees spend their time on the Internet, in the same way that they currently review information about the use of central PBX telephone systems and server computers. Employers are typically concerned about the impact of non-business-related internet surfing and email use on employee productivity and the costs associated with wasted time.

2. Network Bandwidth and Resources: Internet access is not free. Excessive non-business usage of the Internet results in real costs to the agency/entity—for example, the cost to upgrade network resources such as leased lines, routers, disk storage, and printers in order to handle increased load—as well as the cost of wasted time caused by slow network response or unreliable connections. Management needs the tools to rationalize, justify, or apportion the costs of Internet usage based on real-world data.

3. Loss of Confidential Data Agency/entity sensitive information may leak out through email communications. Sensitive information concerning employees, elected officials, sealed bid information, or financial data can easily find its way into an outbound email, whether through intentional efforts or through accidental means. (Example: the user unintentionally hits "Reply All" rather than "Reply.")

4. Potential Legal Liabilities or Negative Publicity: Inappropriate Internet usage may result in legal liabilities and/or negative publicity to the agency/entity. Examples include employees who:

a. Display sensitive material on their workstations or send offensive messages resulting in perceived "hostile environments."

b. Conduct personal business from the Government's server.

c. Visit inappropriate sites allowing the agency's/entity's domain name (e.g., john_doe@yourcompany.com) to be captured, possibly resulting in negative publicity.

5. Exposure to Virus Attacks: The widespread use of the Internet and rapid spread of complex viruses via email has created security issues for government organizations of all sizes. Infected emails can be broadcast to entire networks through gateways and mail servers, thereby halting mission-critical government processes.

How Do You Prevent Internet Abuse?

The Aberdeen Group, a leading computer industry market research, analysis and consulting organization says, *"If employees are left unrestricted by policy and unchecked by monitoring software, then the corporation has exposed itself to significant legal liabilities, probable bandwidth abuse, and employee productivity gaps."* This conclusion, according to the Aberdeen Group, is backed up by reports from the FBI, government and independent research that show employees are the single highest risk and most common cause of network abuse, data loss, and litigation.

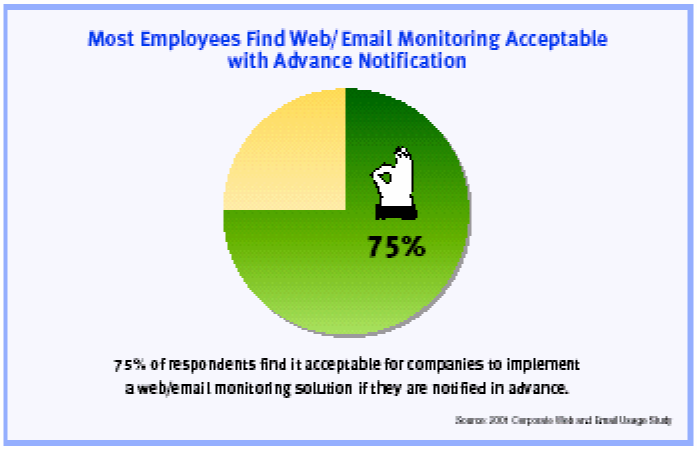
The first step to controlling and managing web and email usage is having an Internet Acceptable Usage Policy. An IAUP establishes what is permissible when using company resources to access the Internet. Active promotion, training, and enforcement of the policy is integral to successful implementation. To ensure policy compliance and receive feedback on implementation, you'll also need a tool that can provide monitoring and reporting of actual usage.

Does an IAUP Work?

Government organizations who have implemented an IAUP and monitoring tools have reported significant improvements in network speed and avoidance of costly network bandwidth upgrades. The results are primarily due to the dramatic reduction in inappropriate usage once a policy has been announced and distributed within the organization. Also, as a direct consequence of having an IAUP, employee time is used more constructively as recreational Internet use is reduced or eliminated and the organization receives increased protection in cases of legal liability.

By Monitoring Are You Infringing on Employees' Rights to Privacy?

Employees say it's OK to monitor. In numerous surveys, including the *2001 Corporate Web and Email Usage Study* by NFO In Depth Interactive, 75% of respondents find it acceptable for companies to implement a web/email monitoring solution if they are notified in advance. You should reinforce to users that the PC on their desk, just like the telephone, is a business tool paid for by your company. Telephone bills are reviewed to ensure appropriate usage and billing in the same manner Internet access may be monitored, per policy, to ensure proper usage.



Most Employees Find Web/ Email Monitoring Acceptable with Advance Notification

75% of respondents find it acceptable for companies to implement a web/email monitoring solution if they are notified in advance.

Source: 2001 Corporate Web and Email Usage Study

Monitoring Legal?

In a recent *Journal of Biolaw & Business* article entitled, "Employer Guidelines for Workplace Email and Internet Policies," employment law attorneys Mark E. Schreiber and Emily C. Ehl state the following: *"A basic issue in employee rights cases is whether employees have a right to privacy in their email messages. As with most invasion of privacy cases, the core issue is whether an employee had a reasonable expectation that his or her personal email messages or web traffic would be private from his employer (and in the case of a public employer, whether the workplace search is sufficiently tailored under the fourth amendment to the government's interest in the efficient and proper operation of the job site). As the few reported cases indicate, employees have had little success in suing their employers for invasion of privacy when their employers accessed their emails or Internet activity, especially where the company had a clear and well disseminated email and Internet policy in place."*

How Can Inappropriate Internet Usage Lead to a Sexual Harassment Lawsuit?

There are two kinds of offenses which can lead to sexual harassment lawsuits in the workplace. Quid pro quo involves a required exchange, such as: "You must sleep with me to get a promotion." But most complaints are in what lawyers call the hostile work environment category. These claims, says Deborah Haude, an attorney with Chicago's Winston & Strawn, involve *"unwelcome sexual conduct, whether verbal or physical, off-color cartoons, or whatever, that intimidates or interferes with the work of a reasonable person."* When an individual downloads sexually explicit material onto his or her desktop, for example, others finding the material offensive could make a case for a hostile work environment. If the company lacks a strict Internet policy prohibiting visits to adult sites, the company may be opening itself up to potential litigation.

What Are Your Actual Risks?

Accessing adult-oriented sites aren't the only risks . Other risks include copyright violations, gambling and posting false information on the Internet about others. In general, Agency Heads/Elected Officials can be held liable for something an employee does, using government resources on the Internet.

What Are the Steps for Implementing an Effective IAUP and Preventing a Hostile Workplace?

Establish a *written* policy. You may use the one included in this guide as a template for creating your own ***(make sure to have it reviewed by your own legal staff and management).***

Post your policy and give each person a copy to be signed and with a returned acknowledgment of having read it (perhaps an email confirmation if the policy is posted on your Intranet). Make sure your policy lists the person or people at your company to whom policy violation claims should be reported. Select these people thoughtfully.

Vigorously promote and enforce your policy. Publicizing your policy through seminars or informal sessions with workers is a great way to telegraph your intent to enforce it. Use Internet monitoring and reporting software to ensure compliance.

What Happens if You Don't Have an IAUP?

If you find your employees are abusing their Internet privileges, but you don't have an IAUP, you can still take action against the offenders. As a agency resource, Internet access along with government computers are subject to general policy and discretionary usage. However, if managers are aware that their employees are visiting adult-oriented web sites or other inappropriate activity, but do not take action, you could be at risk for a hostile-workplace complaint. Even if you win in court, you'll be the victim of scathing publicity and you could be forced to pay heavy legal fees while losing many hours preparing for litigation. To prevent any uncertainty and to protect yourself in the future, distribute an IAUP to your users and implement a monitoring tool.

Do You Have to Monitor Each Individual?

Yes. If you publish a policy that states employees can be monitored and you don't enforce it, you may open yourself up to increased legal liability in cases of a complaint. The common sense approach says the most important element in an effective IUP program is the policy itself. Once that is created and promoted, a periodic review of usage reports using a monitoring tool should be sufficient to provide feedback on the effectiveness of your policy compliance. If you notice repeated attempts to access banned sites, take action according to your policy. If there is a suspected problem or if you need to investigate a specific complaint, you have the ability to do so with a monitoring tool. Using the common sense approach to monitoring, you can make the job of policy compliance a non-burdensome responsibility while reducing legal liability.

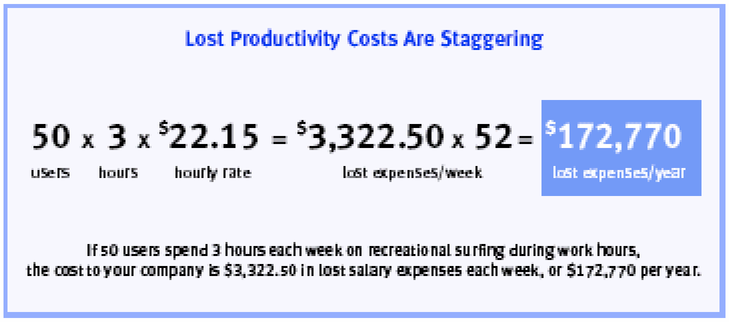
Can You Use Block Lists in Lieu of Monitoring?

Employment lawyer and litigation expert, Mark E. Schreiber, a partner with Palmer & Dodge LLP in Boston states:

"Issues with this approach include, for example, who determines the sites to be blocked? How often will the company have to update these lists? How many sites are to be added to these lists daily? How much storage space do these lists require? Another Internet filtering approach is a technology that automatically builds and maintains a list of restricted web sites without the need for continuous third party updates. With this approach, network managers can set their own criteria for blocking web sites by creating a 'Suspect Dictionary' containing keywords. Whenever a user attempts to access a site containing one of the keywords specified in the 'Suspect Dictionary,' the filtering solution will automatically block access to the suspect site and add the web site address to its list of restricted sites. This technology can also automatically verify the 'suspect' site based on the actual text on the web page, in addition to the name or URL 'header.' New software programs give an employer the ability to automatically forward offensive emails to an administrator or department manager and/or to send warnings to employees that they have violated company policy."

Lost Productivity: How Much Does It Cost

To quantify the mean cost of employee time spent on the Internet you can multiply hours spent online times hourly compensation. Using the US Department of Labor 2001 figures for employer costs for employee compensation (across private, state, and local government) of $22.15 per hour, the following example quantifies your costs:



Lost Productivity Costs Are Staggering

50	x	3	x	$22.15	=	$3,322.50	x	52	=	$172,770
users		hours		hourly rate		lost expenses/week				lost expenses/year

If 50 users spend 3 hours each week on recreational surfing during work hours, the cost to your company is $3,322.50 in lost salary expenses each week, or $172,770 per year.

Internet Usage Policy Template

INTRODUCTION

On the pages that follow, I have laid out some suggestions for a baseline policy and a number of possible modifications to adapt that policy to particular corporate cultures, usage patterns and security needs. A number of public sources were consulted in researching the material for this template, including the Internet Acceptable Usage Policies of the United States Department of Agriculture, Intel Corp., and the federal government's Federal Networking Council. Additional material was suggested by the Business Software Alliance, the Software Publishers Association, and the International Computer Security Association. These organizations maintain substantial reference facilities on their web sites.

Disclaimer

FINALLY, I AM NOT A LAWYER: THIS INTERNET POLICY TEMPLATE IS INTENDED FOR REFERENCE ONLY. SUGGESTIONS HEREIN ARE MEANT TO GIVE GUIDANCE ONLY. SOME OF THESE SUGGESTIONS MAY HAVE LITTLE OR NO BEARING ON YOUR AGENCY'S/ENTITY'S NEEDS. YOUR ORGANAZATION'S INTERNET USAGE AND SECURITY POLICIES SHOULD BE CHECKED CAREFULLY BY A COMPETENT ATTORNEY WHO IS THOROUGHLY FAMILIAR WITH YOUR AGENCY'S SPECIFIC SITUATION, NOT SIMPLY LIFTED VERBATIM.

SUMMARY INTERNET USAGE POLICY PROVISIONS

1. The (insert name) has software and systems in place that can monitor and record all Internet usage.

2. We reserve the right to inspect any and all files stored in private areas of our network in order to assure compliance with policy.

3. Sexually explicit material may not be displayed, archived, stored, distributed, edited or recorded using our network or computing resources.

4. Use of any (insert name) resources for illegal activity is grounds for immediate dismissal, and we will cooperate with any legitimate law enforcement activity.

5. Any software or files downloaded via the Internet into the (insert name) network become the property of the (insert name).

6. No employee may use (insert name) facilities knowingly to download or distribute pirated software or data.

7. No employee may use the (insert name) Internet facilities to deliberately propagate any virus, worm, Trojan horse or trap-door program code.

8. In the interest of keeping the (insert name) well-informed, use of news briefing services like Pointcast is acceptable.

9. Employees with Internet access may not use (insert name) Internet facilities to download entertainment software or games, or to play games against opponents over the Internet.

10. Employees with Internet access may not upload any software licensed to the (insert name) or data owned or licensed by the (insert name) without explicit authorization from the manager responsible for the software or data. The entire Internet Acceptable Usage Policy is attached to this document. Please read the policy and return the Acknowledgment to Human Resources.

INTERNET USAGE POLICY

Overview

(Insert name) provides access to the vast information resources of the Internet to help you do your job and be well-informed. The facilities that provide access represent a considerable commitment of resources for telecommunications, networking, software, storage, etc. This Internet Acceptable Usage Policy is designed to help you understand the expectations for the use of those resources in the particular conditions of the Internet, and to help you use those resources wisely. While we've set forth explicit requirements for Internet usage below, we'd like to start by describing our Internet usage philosophy. First and foremost, the Internet for this (insert name) is a tool, provided to you at significant cost. That means we expect you to use your Internet access primarily for government-related purposes, i.e., to communicate with taxpayers and suppliers, to research relevant topics and obtain useful information (except as outlined below). We insist that you conduct yourself honestly and appropriately on the Internet, and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others, just as you would in any other business dealings. To be absolutely clear on this point, all existing (insert name) policies apply to your conduct on the Internet, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of (insert name) resources, sexual harassment, information and data security, and confidentiality. Unnecessary or unauthorized Internet usage causes network and server congestion. It slows other users, takes away from work time, consumes supplies, and ties up printers and other shared resources. Unlawful Internet usage may also garner negative publicity for the agency and expose the state/county/municipality to significant legal liabilities. Access to electronic communications gives each individual Internet user an immense and unprecedented reach to propagate (insert name) messages and tell our business story. Because of that power, one must take special care to maintain the clarity, consistency and integrity of the (insert name) image and posture. Anything any one employee writes in the course of acting for the (insert name) on the Internet could be taken as representing the (insert name) posture. That is why we expect you to forego a measure of your individual freedom when you participate in electronic communications as outlined below. While our direct connection to the Internet offers a cornucopia of potential benefits, it can also open the door to some significant risks to our data and systems if we do not follow appropriate security discipline. As presented in greater detail below, that may mean preventing machines with sensitive data or applications from connecting to the Internet entirely, or it may mean that certain users must be prevented from using certain Internet features. The overriding principle is that security is to be everyone's first concern. (insert name) employees can be held accountable for any breaches of security or confidentiality including any and all branches. "Document" covers just about any type of file that can be read on a computer screen as if it were a printed page, including the so-called HTML files read in an Internet browser, any file meant to be accessed by a word processing or desktop publishing program or its viewer, or the files prepared for the Adobe Acrobat reader and other electronic publishing tools. "Graphics" includes photographs, pictures, animations, movies or drawings. "Display" includes monitors, flat-panel active or passive matrix displays, monochrome LCDs, projectors, televisions, and virtual-reality tools.

DETAILED INTERNET USAGE POLICY PROVISIONS

A) General

1. The (insert name) has software and systems in place that monitor and record all Internet usage. Our security systems are capable of recording (for each and every user) each World Wide Web site visit and each email message into and out of our internal networks, and we reserve the right to do so at any time. No employee should have any expectation of privacy as to his or her Internet usage. Our managers will review Internet activity and analyze usage patterns and they may choose to publicize this data to assure that (insert name) internet resources are devoted to maintaining the highest levels of productivity.

2. We reserve the right to inspect any and all files stored in private areas of our network in order to assure compliance with policy.

3. The display of any kind of sexually explicit image or document on any (insert name) system is a violation of our policy on sexual harassment. In addition, sexually explicit material may not be archived, stored, distributed, edited, or recorded using our network or computing resources.

4. The (insert name) uses independently-supplied software and data to identify inappropriate or sexually explicit Internet sites. We may block access from within our networks to all such sites that we know of. If you find yourself connected accidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program.

5. The (insert name) Internet facilities and computing resources must not be used to violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province or other local jurisdiction in any material way. Use of any (insert name) resources for illegal activity is grounds for immediate dismissal and we will cooperate with any legitimate law enforcement activity.

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

7. No employee may use (insert name) facilities to download or distribute pirated software or data.

8. No employee may use the (insert name) Internet facilities to propagate any virus, worm, Trojan horse or trap-door program code.

9. Each employee using the Internet facilities of the (insert name) shall identify himself or herself honestly, accurately and completely, when setting up accounts on outside computer systems.

10. Only those employees or officials who are authorized to speak to the media, to analysts or at public gatherings on behalf of the (insert name) may speak/write in the name of the (insert name) in any electronic communications. Where an individual participant is identified as an employee or agent of the (insert name) the employee must refrain from any political advocacy and must refrain from the unauthorized endorsement or appearance of endorsement by the (insert name) of any commercial product or service not sold or serviced by this (insert name), its subsidiaries or its affiliates.

11. The (insert name) retains the copyright to any material posted on the Internet by any employee in the course of his or her duties.

12. Employees are reminded that it is inappropriate to reveal confidential information, and any other material covered by existing (insert name) secrecy policies and procedures on the Internet. Employees releasing such confidential information— whether or not the release is inadvertent — will be subject to the penalties provided in existing (insert name) policies and procedures.

13. Use of (insert name) Internet access facilities to commit infractions such as misuse of (insert name) assets or resources, sexual harassment, unauthorized public speaking and misappropriation of intellectual property are also prohibited by general (insert name) policy and will be sanctioned under the relevant provisions of the personnel handbook.

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

15. In the interest of keeping employees well-informed, use of news briefing services like Pointcast is acceptable, within limits that may be set by each department's activities.

16. Employees may use their Internet facilities for non-business research or browsing during meal time or other breaks, or outside of work hours, provided that all other usage policies are adhered to.

17. Employees with Internet access must take particular care to understand the copyright, trademark, libel, slander, and public speech control laws of all countries in which this governmental agency maintains a business presence, so that our use of the Internet does not inadvertently violate any laws which might be enforceable against us.

18. Employees with Internet access may not use (insert name) Internet facilities to download entertainment software or games, or to play games against opponents over the Internet.

19. Employees with Internet access may not use (insert name) Internet facilities to download images or videos unless there is an express business-related use for the material.

20. Employees with Internet access may not upload any software licensed to the (insert name) or data owned or licensed by the (insert name) without the express authorization of the manager responsible for the software or data.

B) Technical

1. User IDs and passwords help maintain individual accountability for Internet resource usage. Any employee who obtains a password or ID for an Internet resource from (insert name) must keep that password confidential. (insert name) policy prohibits the sharing of user IDs or passwords obtained for access to Internet sites.

2. Employees should schedule communications-intensive operations such as large file transfers, video downloads, mass e-mailings and the like, for off-peak times.

3. Any file that is downloaded must be scanned for viruses before it is run or accessed.

C) Security

1. The (insert name) has installed an Internet firewall to assure the safety and security of the agency's networks. Any employee who attempts to disable, defeat, or circumvent any security facility will be subject to immediate dismissal.

2. Files containing sensitive Company data, as defined by existing data security policy, that are transferred in any way across the Internet must be encrypted.

3. Only those Internet services and functions with documented business purposes for this agency will be enabled at the Internet firewall.

Acknowledgment

I acknowledge that I have received a written copy of the Internet Acceptable Usage Policy for (Agency/Entity NAME). I understand the terms of this policy and agree to abide by them. I realize that the (Agency/Entity NAME) security software may record and store for management use the electronic email messages I send and receive, the Internet address of any site that I visit and any network activity in which I transmit or receive any type of file. I understand that any violation of this policy could lead to my dismissal from employment or even criminal prosecution. I you have any question regarding this policy or any situation not specifically addressed in this policy, see your supervisor or the (insert name) Personnel Director. This policy is subject to revision. (Insert name) will adequately post revisions, but it is the user's responsibility to ensure that his/her use of the (Insert name) computing and communication resources conforms to current policy**.**

____
Signature

____
Name (Printed)

____
Date