



Ensuring your success

Suggested Guidelines for Internet and E-mail Use

DURHAM AND BATES AGENCIES, INC.

Addressing Internet and E-mail Use

To reduce potential liability for your company, you should develop a clear e-mail and/or internet policy. This compilation is intended to assist your business in addressing its need for internet and e-mail use policies. As always, the advice and consent of your employment attorney is highly recommended.

I. Overview: Internet and E-mail Policy

- **The Purpose of an Internet and E-mail Use Policy**

The primary purpose of the policy is to reduce employees' expectations of privacy and define the boundaries of employee conduct with respect to e-mail and the Internet. When clearly communicated, the policy protects business because it defines acceptable internet and e-mail behavior. In addition to eliminating questions around appropriate use, a strong policy mitigates risk of liability by reducing employees' presumption of privacy. When employees understand the company's position on internet and e-mail use, the risk of policy transgression is reduced.

- **Important Elements to Consider in Implementing an Internet/e-mail Use Policy**

When designing an internet and e-mail use policy, it must be tailored to suit the business needs of your company, reasonable expectations of your employees and a balance of other interests.

- **Clearly Spell Out Privacy Expectations**

Depending upon your business' position on internet/e-mail monitoring, the policy must be clear in the care and degree of employee privacy practiced. For instance, if employees should not have a reasonable expectation of privacy, the content should clearly state that the e-mail/internet system is the property of the employer, and management reserves the right to monitor use of the system at any time, at its sole discretion, with or without notice.

- **Distribute To All Employees**

No matter what the specifics of your policy, however, the final policy should be given to all employees and placed in employee manuals. Employee signatures confirming receipt of policies are especially prudent.

II. Creating an Internet/e-mail Use Policy - Specific Content Checklist

The below specific guidelines are written to help your business design an appropriate internet/e-mail use policy to serve its particular needs. Other elements could also be contained within the policy, subject to your specific needs.

- The policy could notify employees that the systems are solely (or if desirable primarily) for business use, and that the company reserves the absolute right to review, audit and disclose all matters sent over the system or placed into its storage. In addition to the written notification in the handbook or other written materials, ongoing notice to employees can be provided by programming a message that would appear on the employee's monitor each time the employee accesses the system. It would also specify that the employer reserves the right to access any messages or information entered into the system.
- The policy could specify that the system should not be used to communicate any improper communications, e.g., messages which are derogatory, defamatory, obscene or, inappropriate.
- To reduce any reasonable expectation of privacy, the policy should not limit your reasons for monitoring the system. Any limitation could be argued to restrict the scope of the employee's consent to the monitoring. A more cautious approach would be to establish a business purpose that would be articulated in connection with any monitoring so as to defeat any possible expectation of privacy.
- Consistent with the prohibition against non-business use of the system, the policy could be subject to the employer's no-solicitation rule as could all other means of intra-company communication. Such a rule would encompass any solicitation, whether for charitable, personal, business or union organizing purposes. An alternative would be to allow access to an electronic bulletin board (that can be viewed by all employees) for solicitation and/or personal messages.
- To further diminish the reasonable expectation of privacy, the policy could contain a warning that the mere deletion of a message or file may not fully eliminate the message from the system.
- The policy could be accompanied by a form which employees could be required to sign acknowledging the business' absolute right to access the system's information. Requiring employees to sign the form will further eliminate any expectation of privacy in the information transmitted and could prevent an employee from claiming that he/she was unaware of the policy.
- The policy could make clear that a violation of the policy may result in disciplinary action up to and including discharge from employment. The employer could also specify that any abuse of the system, e.g., inappropriate content, accessing files beyond those necessary by the employee (and/or use of the system for personal reasons) will result in disciplinary action.
- Notwithstanding a strong policy statement permitting monitoring, actual monitoring of electronic communications could be limited to situations where such monitoring is necessary to protect your business purposes. The least intrusive method of monitoring could be utilized and excessive intrusion into personal communications should be avoided.
- In order to reduce the potential for defamation and/or invasion of privacy claims, disclosure of the information obtained from the system could be limited to those who have a legitimate need to know.

III. A Sample Internet and E-mail Use Policy

E-mail and Internet Access

Purpose

To define the proper use of electronic mail (e-mail) and Internet services at Employer.

Policy

Employer is committed to providing an environment that encourages the use of computers and electronic information as essential tools to support Employer's business. It is the responsibility of each employee to ensure that this technology is used for proper business purposes and in a manner that does not compromise the confidentiality of proprietary or other sensitive information. This policy supplements, and should be read in conjunction with, Employer's policies regarding "Corporate Communications"; "Confidentiality"; and "Use of the Company's Communications Systems."

Coverage

All users of Employer's computer systems.

E-Mail Procedures

- All e-mail correspondence is the property of Employer.
- Employee e-mail communications are not considered private despite any such designation either by the sender or the recipient.
- Messages sent to recipients outside of Employer, if sent over the Internet and not encrypted, are not secure.
- Employer reserves the right to monitor its e-mail system - including an employee's mailbox - at its discretion in the ordinary course of business. Please note that in certain situations, Employer may be compelled to access and disclose messages sent over its e-mail system.
- The existence of passwords and "message delete" functions do not restrict or eliminate Employer's ability or right to access electronic communications.
- Employees shall not share an e-mail password, provide E-mail access to an unauthorized user, or access another user's e-mail box without authorization.
- Employees shall not post, display or make easily available any access information, including, but not limited to, passwords.
- Offensive, demeaning or disruptive messages are prohibited. This includes, but is not limited to, messages that are inconsistent with Employer's policies concerning "Equal Employment Opportunity"; and "Sexual Harassment and Other Unlawful Harassment."
- Messages sent to all e-mail users require prior approval by an appropriate member of Employer.

Any employee who violates this policy shall be subject to discipline, up to and including discharge.

III. A Sample Internet and E-mail Use Policy (cont.)

Internet Procedures

- Employer's network, including its connection to the Internet, is to be used for (or primarily for) business - related purposes only and not for personal use (or primarily for business - related purposes). Any unauthorized use of the Internet is strictly prohibited. Unauthorized use includes, but is not limited to: connecting, posting, or downloading pornographic material; engaging in computer-"hacking" and other related activities; attempting to disable or compromise the security of information contained on Employer's computers (or otherwise using Employer's computers for personal use).
- Internet messages should be treated as non-confidential. Anything sent through the Internet passes through a number of different computer systems, all with different levels of security. The confidentiality of messages may be compromised at any point along the way, unless the messages are encrypted.
- Because postings placed on the Internet may display Employer's address, make certain before posting information on the Internet that the information reflects the standards and policies of Employer. Under no circumstances shall information of a confidential, sensitive or otherwise proprietary nature be placed on the Internet.
- Subscriptions to new groups and mailing lists are permitted when the subscription is for a work-related purpose. Any other subscriptions are prohibited.
- Information posted or viewed on the Internet may constitute published material. Therefore, reproduction of information posted or otherwise available over the Internet may be done only by express permission from the author or copyright holder.
- Unless the prior approval of management has been obtained, users may not establish Internet or other external network connections that could allow unauthorized persons to gain access to Employer's systems and information. These connections include establishment of hosts with public modem dial-ins, World Wide Web home pages and File Transfer Protocol (FTP).
- All files downloaded from the Internet must be checked for possible computer viruses. If uncertain whether your virus-checking software is current, you must check with an authorized Information Systems Representative before downloading.
- Offensive, demeaning or disruptive messages are prohibited. This includes, but is not limited to messages that are inconsistent with Employer's policies concerning "Equal Employment Opportunity"; and "Sexual Harassment and Other Unlawful Harassment."

Any employee who violates this policy shall be subject to discipline, up to and including discharge.

IV. A Sample Acknowledgement of Internet and E-mail Use Policy

Acknowledgment of E-mail and Internet Use Policy

- *As an employee of Employer, I understand that the confidentiality and protection of Employer's information is of the utmost importance. I have read and understand Employer's Policy on acceptable use of e-mail and Internet access.*
- *If I receive a password for access to e-mail, the Internet or any other system of electronically - stored computer information, I will use it only for authorized purposes. I agree not to use a code, access a file or retrieve any stored communication other than where explicitly authorized unless there has been prior clearance by an authorized representative of Employer. I will notify Information Systems immediately if I believe that another person may have unauthorized access to my password.*
- *I understand that all information stored in, transmitted or received through Employer's systems of printed or computer information is the property of Employer, and is to be used only for job-related purposes. I further understand that authorized representative of Employer may monitor the use of Employer's systems of printed or computer information from time to time to ensure that such use is consistent with Employer's policies and interests. Further, I am aware that use of an Employer-provided password or code does not in any way restrict Employer's right or ability to access electronic communications.*
- *I am aware that any violation of Employer's e-mail or Internet Access Policy may subject me to disciplinary action, up to and including discharge from employment.*

Employee Signature

Date

Supervisor Signature

Date