



EMPLOYEE COMPUTER, E-MAIL, AND INTERNET USAGE POLICY

Included:

Overview

Dos and Don'ts Checklist

Sample Computer, E-mail, and Internet Usage Policy

1. Overview

Every business that uses computers should have a written computer, e-mail, and internet usage policy. These policies are sometimes also called “acceptable use policies,” “acceptable usage policies” or “AUPs.” The temptation to surf the web or compose personal e-mails is hard to resist for even the most conscientious of employees, and these practices waste significant company money and time. Moreover, a pattern of careless computer use can have significant risks for a business, in both the short term and farther down the road.

A well-crafted computer, e-mail, and internet usage policy will not only set expectations for incoming employees, but will also protect your company from allegations ranging from copyright infringement to hostile work environment. The policy will also guard against more immediate dangers, like the unthinking download of a computer virus or of tools that could interfere with system security.

The enclosed policy should prove useful to your business and, if you follow the suggestions provided, can provide the framework for a complete set of information management policies. Your business will be able to draw on its technological resources without sacrificing either security or efficiency.

2. Dos & Don'ts Checklist

Creating an employee computer, internet, and e-mail usage policy is the first of many steps in establishing a healthy, professional, and dispute-free workplace. The following tips will provide additional guidance about protecting your company and its electronic communications:

- Computer systems are imperfect and, even if your employees are careful, confidential or sensitive information may be lost or made public. Protect your content with encryption software and regular archiving of important electronic materials. Critical data should be backed up or duplicated and stored securely.
- Make sure your company's discrimination and sexual harassment policies are included in your e-mail policy (like the policy contained in this packet). Employees tend to be more casual with their remarks in an electronic setting, and it's important to emphasize that inappropriate comments will not be tolerated in any work-related forum.
- Instruct all company employees about the importance, security, and protection of e-mail information. Wrongful disclosure can happen at any level of your organization. If sensitive information needs to be exchanged, consider a phone call or a face-to-face meeting rather than risking privacy in a written document.
- Be reasonable in your policies. Many present-day employees work long hours, leaving their houses before dawn and returning well into the night. For the sake of workplace morale and staff retention, you should allow some electronic communication between employees and their family members.
- An important part of maintaining company files is recognizing when records are no longer needed for your business. This is true for both paper and electronic documents. It's a good idea to draft policies and procedures explaining when and how to dispose of dated and private materials.

- Every person employed by your company should review and sign your policy. This includes new, old, temporary, and permanent employees, managers, supervisors, full-time professionals, part-time staff, independent contractors, and freelancers.
- Allow your employees ample time to review and sign the policy. This will reduce the likelihood, or at least the efficacy, of a claim that an individual did not understand the policy's terms.
- Review the computer, e-mail, and internet usage policy carefully. One size may not fit all.

You can use these suggestions and the enclosed model to create a thorough computer, e-mail, and internet usage policy, a policy that will protect your company from both internal and external risks. You will have created a document that can be used with each new employee of your business, and that may shield confidential information from inadvertent disclosure or destruction.

3. Computer, E-mail, and Internet Usage Policy Instructions

The following provision-by-provision instructions will help you understand the terms of your computer, e-mail, and internet usage policy. Please review the entire policy before starting the step-by-step process.

- **Section 1: Access and Review of E-Mail Communications and Internet Usage.** Explains that employees should not expect any e-mails sent through the company computer system to be private. In other words, all e-mails sent using work technology, whether for business or for personal matters, can be retrieved and reviewed by the company.
- **Section 2: E-Mail Etiquette.** Reiterates the general rule that employees should use caution in drafting and forwarding e-mails.
- **Section 3: Storing and Deleting E-Mail Messages.** As the heading indicates, the company's policy about keeping and deleting e-mails is detailed in this section. Specifically, to advance company goals of efficiency and security, employees are encouraged to get rid of e-mails that aren't required for current (or anticipated) business matters.
- **Section 4: Subscriptions to Mailing Lists and Discussion Groups.** States that any e-mail subscriptions or discussion groups to which an employee belongs must be related to his or her job.
- **Section 5: Permitted and Prohibited Uses.** Taken as a whole, this section describes what an employee can and cannot do using company technology. The examples provided in the subsections should not be considered exhaustive: if there are specific acts that you want to allow or prevent, you can add descriptions of those acts to the appropriate paragraphs.
- **Section 6: Computer System Security.** Although many of this policy's clauses are aimed at preventing employees from sending or reviewing prohibited materials, companies should also be concerned about less direct threats to their technology systems. More specifically, this section warns employees that their actions can endanger the general security of the company, calling particular attention to the dangers posed by computer viruses, unauthorized log-ins, and individual software downloads.

- **Section 7: Confidentiality of Communications.** This final section emphasizes that an employee's duties to protect the company's confidential information apply to cyberspace. Indeed, particular attention may be required online, where the rules of communication may seem to be more relaxed.

A company that uses the tools provided in this package can clarify an employee's obligations and duties regarding electronic communication. This knowledge and awareness can limit careless disclosures and protect your business: the greater the employee's understanding of the consequences of a misstep, the more seriously they will take their obligations. A firewall can protect your company from outside threats to its information; a good policy on computer, internet, and e-mail usage will protect you from internal dangers as well.

DISCLAIMER

LegalZoom is not a law firm. The information contained in the packet is general legal information and should not be construed as legal advice to be applied to any specific factual situation. The use of the materials in this packet does not create or constitute an attorney-client relationship between the user of this form and LegalZoom, its employees or any other person associated with LegalZoom. Because the law differs in each legal jurisdiction and may be interpreted or applied differently depending on your location or situation, you should not rely upon the materials provided in this packet without first consulting an attorney with respect to your specific situation.

The materials in this packet are provided "As-Is," without warranty or condition of any kind whatsoever. LegalZoom does not warrant the materials' quality, accuracy, timeliness, completeness, merchantability or fitness for use or purpose. To the maximum extent provided by law, LegalZoom, its agents and officers shall not be liable for any damages whatsoever (including compensatory, special, direct, incidental, indirect, consequential, punitive or any other damages) arising out of the use or the inability to use the materials provided in this packet.

COMPUTER, E-MAIL AND INTERNET USAGE POLICY

This document sets forth [Company's] (the "Company") policies with regard to computer, e-mail, and Internet usage, including access to, review or disclosure of e-mail messages sent or received by Company employees, and Internet access and usage. The Company reserves the right to modify or update these policies at any time. **Use of the computer system, e-mail system, or the Internet in violation of these policies or other Company policies can result in disciplinary action, including termination of employment.**

The Company computer system, e-mail system, and Internet access (collectively called the "Computer System" in this document) are provided to employees at the Company's expense to assist them in carrying out Company business and performing their job responsibilities and duties.

The Company owns, maintains, and is responsible for the Computer System. In the course of their jobs, employees may use the Computer System to communicate internally with co-workers or externally with clients, consultants, vendors, and other business acquaintances. The Company provides its employees with the Computer System to facilitate business communications and to enhance employee productivity. As with the telephone, there may be occasion to use the Computer System for personal purposes. Personal use is permitted if it does not interfere with job performance, consume significant resources, give rise to more than nominal additional costs, or interfere with the activities of other employees. Under no circumstances shall the Computer System be used for personal financial gain, to solicit others for activities unrelated to the Company's business, or in connection with political campaigns or lobbying.

1. Access and Review of E-Mail Communications and Internet Usage

The Company treats all messages sent, received, or stored in its systems as Company messages.

The Company