Company Internet and Email Policy

An effective internet and email policy that helps employees understand what is expected of them regarding how they use their devices for work is a must for employers and employees. You want to go on record to define what employees can do from work-provided or employee-owned devices that are used by or involve your employees, your workplace, or your company.

With nearly 80% of the people in the U.S. accessing social media, guidance about what employees can say and share has become more important.1﻿ Most employees don't mind guidelines because they don't want to act inappropriately or cross a line unawares. So, the development of a fair, understandable, and sensible policy along with thorough training should be a top priority.

Consider using this sample internet and email policy to provide clear guidance to your employees about what constitutes appropriate internet and email use at work. Adapt it to suit the needs of your culture and the environment you want to provide employees at work. To be sure of legalities in your area and in your industry, please consult an attorney.

Sample Internet and Email Policy for Employees

Voicemail, email, and internet usage assigned to an employee's computer or telephone extensions are solely for the purpose of conducting company business. Some job responsibilities at the company require access to the internet and the use of software in addition to the Microsoft Office suite of products.

Only people appropriately authorized, for company purposes, may use the internet to access and download additional software. This authorization is generally exclusive to decisions that the information technology (IT) department makes in conjunction with human resources.

Software Access Procedure

Software needed in addition to the Microsoft Office suite of products must be authorized by your manager and downloaded by the IT department. If you need access to software or websites not currently on the company network, talk with your manager and consult with the IT department to explain what returns you expect to receive from the product.

All reasonable requests that are not considered a network risk will be considered. The purpose of this policy is not to restrict employee access to products that will make you more productive. Rather, the goal is to minimize the risk to the organization's network.

Company-Owned Equipment

Any device or computer including, but not limited to, desk phones, smartphones, tablets, laptops, desktop computers, and iPads that the company provides for your use, should be used only for company business. Keep in mind that the company owns the devices and the information on these devices. If you leave the company for any reason, the company will require that you return the equipment on your last day of work.

You may use personal electronic devices that are not connected to the company network to access any appropriate internet site during breaks and lunch.

Internet Usage

Internet use on company time or using company-owned devices that are connected to the company network is authorized to conduct company business only. This limits the possibility of breaches of the security of confidential company information.

Internet use also creates the possibility of contamination to our system via viruses or spyware. Spyware allows unauthorized people outside of the company potential access to company passwords and other confidential information.

Removing such programs from the company network requires IT staff to invest time and attention that is better devoted to making technological progress. For this reason, and to assure the appropriate use of work time, we ask staff members to limit internet use.

Additionally, under no circumstances may company-owned computers or other electronic equipment, including devices owned by the employee, be used on company time at work to obtain, view, or reach any pornographic, or otherwise immoral, unethical, or nonbusiness-related internet sites. Doing so can lead to disciplinary action up to and including termination of employment.

Social Media

Your employer understands that part of what you do in social media is outreach that recruits new employees and enhances our company brand. Many employees even have social media responsibilities in their job descriptions, including social media marketers, tech support, and recruiters.

Your employer also understands that the relationship of our employees to an online world that you spend time in 24/7 can lead to the blurring of work time and off-work time. We strongly encourage you to limit the use of social media to work-related content and outreach during work hours.

Additionally, you are prohibited from sharing any confidential or protected information that belongs to or is about the company. You are strongly encouraged not to share disparaging information that places your company or co-workers in an unfavorable light.

The company's reputation and brand should be protected by all employees. The lives and actions of your co-workers should never be shared online. Please note the preferences of fellow employees—for example, get permission from those who are parents before you use the name of their children online.

In social media participation from work devices or during working hours, social media content that discriminates against any protected classification including age, race, color, religion, gender, national origin, disability, or genetic information is prohibited.

It is our company policy to also include sexual preference, gender identity, and weight under discrimination protection. Any employee who participates in social media and violates this policy will be dealt with according to the company harassment policy.

Email Usage at the Company

Email is to be used for company business only. Confidential company information must not be shared outside of the company, without authorization, at any time. You also are not to conduct personal business using the company computer or email.

Please keep this in mind, also, as you consider forwarding nonbusiness emails to associates, family, or friends. Nonbusiness related emails waste company time and attention.

Viewing pornography, or sending pornographic jokes or stories via email, is considered sexual harassment and will be addressed according to our sexual harassment policy. Immediate termination is the most frequent disciplinary action that the company may take in these cases.

Emails That Discriminate

Any email content that discriminates against any of the previously mentioned protected classifications is prohibited. Any employee who sends an email that violates this policy will be dealt with according to the harassment policy.

These emails are prohibited at the company. Sending or forwarding discriminatory emails will result in disciplinary action that may lead to employment termination.

Company Owns Employee Email

Keep in mind that the company owns any communication sent via email or that is stored on company equipment. Management and other authorized staff have the right to access any material in your email or on your company computer at any time. Please do not consider your electronic communication, storage, or access to be private if it is created or stored on work systems.

If you need additional information about the meaning of any of this communication, please reach out to your manager or the human resources staff for clarification.