

## **Sample Office Internet Policy**

Modify the contents of this document as needed to meet local ordinances and established laws in your area. This document is not meant to replace other legal and binding pre-existing documentation. It is meant to be a starting point only. Print it out and have it signed by all employees that may come into contact with any information assets in your department. Store in a secure location and review with your employees annually. Reviewing and renewing annually will allow you to modify the contents to reflect your ever changing security issues.

What follows is a Sample Office Internet Policy.

## **Internet Usage**

Internet use, on office equipment, is authorized to conduct Company business only. Internet use brings the possibility of breaches to 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 the Office, potential access to passwords and other confidential information.

Removing such programs from the Office network requires IT staff to invest time and attention that is better devoted to progress. For this reason, and to assure the use of work time appropriately for work, we ask staff members to limit Internet use.

Additionally, under no circumstances may Office computers or other electronic equipment be used to obtain, view, or reach any pornographic, or otherwise immoral, unethical, or non-business-related Internet sites. Doing so can lead to disciplinary action up to and including termination of employment.

## **Email Usage at the Office**

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

Please keep this in mind, also, as you consider forwarding non-business emails to associates, family or friends. Non-business related emails waste office 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.

## **Emails That Discriminate**

Any emails that discriminate against employees by virtue of any protected classification including race, gender, nationality, religion, and so forth, will be dealt with according to the harassment policy. These emails are prohibited at the office. Sending or forwarding non-business emails will result in disciplinary action that may lead to employment termination.

## **The Office Owns Employee Email**

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

## **P2P networks**

Participation in P2P (peer to peer) networks like Kazza, Mirc, Morpheus, etc is strictly prohibited. Files transferred to and from the office can subject the office to copyright infringement lawsuits as well as prosecution of the offending individual. P2P networks are also a known source of Trojans and viruses. Any program that connects your computer to another group of computers for the purpose of exchanging files should be approved by your supervisor or IT staff.

## **Use during Breaks, Lunch, and After Hours**

This policy extends to all use of office digital equipment during all hours of the day and night. This policy also applies to any personal computing devices, laptops, PDA's, etc that may be connected to the Office network.

---

Employee

---

Date