Model Computer System Policy

Raymond L. Hogge, Jr.
Hogge Law
Attorneys and Counselors at Law
500 E. Plume Street, Suite 800
Norfolk, Virginia 23510
(757) 961-5400

February 10, 2014

DISCLAIMER: This policy is intended solely for informational purposes and is not offered as legal advice. This policy may or may not be appropriate for a particular employer. Consult qualified legal counsel for assistance in drafting a policy suitable for the needs of your organization.

Our Computer System

{EMPLOYER} maintains a computer system including computer equipment, a computer network, an e-mail system, and an internet access system. Only authorized employees are permitted to use this system, and only to the extent expressly authorized by management. Use of our computer system for personal purposes, or in any way that is unlawful or inconsistent with the policies of the practice, is strictly prohibited.

Practice Property

The computer system, and all data that is composed, saved, stored, transmitted, or received on it, is the property of the {EMPLOYER}. Such data constitutes official business records, may be intercepted, accessed and inspected by management at any time and by any means, and is subject to disclosure by the practice to law enforcement officials. Consequently, employees should always ensure that the information contained in e-mail messages and elsewhere on our computer system is accurate, appropriate, ethical, and lawful.

Virus Protection

Our computer system uses antivirus software which automatically scans all e-mail and other data for computer viruses, malware, and other security threats. Employees are strictly prohibited from tampering or disabling this software. Employees also are responsible for notifying management immediately in the event a workstation displays a warning that the antivirus software may be disabled or less than fully functional. In the event the antivirus software detects a security threat at a workstation, the software will display a warning at the workstation. In the event you see such a warning, immediately stop using the workstation and notify a member of management.

Personal Electronic Devices and Storage Media

No antivirus software can detect every security threat. Therefore, as a security policy, employees are strictly prohibited from connecting personal electronic devices to our computer system. Such personal electronic devices include, but are not limited to, laptop computers, tablet computers (including but not limited to iPads), smartphones (including but not limited to iPhones), and electronic music players (including but not limited to iPods). Employees likewise are strictly prohibited from inserting personal electronic storage media, including but not limited to external hard drives, flash drives, memory cards, DVD's, CD's, and floppy disks, into any drive on our computer system.

Health and Safety

All employees should use the computer system in a manner that promotes a healthy and safe work environment. The following specific guidelines should be observed.

- Keyboards, monitors and mouse pads should be placed in an ergonomically appropriate position. If you are unsure of the proper position for your keyboard, monitor, or mouse pad, or if its placement causes you discomfort, you should promptly notify management.
- Always use all safety devises, such as wrist supports, provided to you. If for any reason you do not wish to use them, you should consult management.
- You should promptly alert management in the event you experience any pain, numbness, tingling, or other unusual sensations in your hands, wrists or arms while using the computer system. These symptoms may indicate you are at risk for carpal tunnel syndrome.
- Never allow clothing, paper, or other flammable objects to come in contact with the wires and cables to your workstation. Doing so may create a fire hazard.
- Never place water, coffee, soda, or any other liquid where it can spill onto your workstation. Such a spill, in addition to damaging the equipment, can create a risk of electric shock.

The preceding guidelines are not exhaustive. You should always exercise good judgment and common sense in the use of our computer system, and should immediately report to management anything you suspect may pose a health or safety risk.

Accommodation to Disabilities

In the event you have a disability which requires an accommodation in order for you to use our computer system, please notify {PERSON OR OFFICE}. In accordance with the practice's commitment to equal opportunity employment, a reasonable accommodation may be provided.

Protection of Intellectual Property Rights

{EMPLOYER} purchases licenses for the use of various computer software for business purposes and does not own the copyright to this software or its related documentation. Unless authorized by the software developer, we and our employees do not have the right to reproduce

such software for use on more than one computer. Accordingly, employees may only use licensed software on local area networks or on multiple machines according to the software license agreement, and the illegal duplication of software or its documentation is prohibited.

The unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material on our computer system is prohibited. As a general rule, if an employee did not create material, does not own the rights to it, or has not gotten authorization for its use, it should not be put on the computer system. Employees are responsible for ensuring that the person sending any material via our computer system has the appropriate distribution rights.

Prohibited Conduct

Our computer system may not be used for personal purposes. Its use to solicit others for commercial ventures, religious activities, political causes, outside organizations, or other nonbusiness matters is prohibited.

{EMPLOYER} strives to maintain a workplace free of harassment and sensitive to the diversity of its employees. Therefore, we prohibit the use of our computer system in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is not allowed. Other such misuse includes, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassment or showing disrespect for others.

The following are other examples of conduct involving the use of our computer system which is prohibited:

- Sending an anonymous e-mail message.
- Sending or posting a discriminatory, harassing, or threatening message or image.
- Sending or posting a message that defames or slanders an individual or company.
- Sending or posting a message that disparages an individual's or company's products or services.
- Sending or posting a message or material that could damage the company's image or reputation.
- Sending or posting a chain letter, solicitation, or advertisement not related to business purposes or activities.
- Sending or posting confidential material, trade secrets, or proprietary information outside of the company.
- Using the system to engage in any illegal activity.
- Using the system for personal gain.
- Using the system for unauthorized transactions that may incur a cost to the company.
- Stealing, using, or disclosing someone else's code or password without authorization.
- Attempting to break into the computer system of another individual or company.
- Copying or downloading software and electronic files without permission.
- Violating copyright law or any software license in connection with the company's computer system.
- Failing to observe licensing agreements.

- Intentionally or carelessly transmitting a virus or introducing it into our system or any other system.
- Participating in the viewing or exchange of pornography or obscene materials.
- Passing off a personal view as representing that of the company.
- Jeopardizing the security of the computer system.
- Failing or refusing to cooperate with a company investigation involving the computer system.

Monitoring

To ensure compliance with this and other policies of the practice, usage of the computer system, including e-mail and internet usage, may be monitored. This monitoring may occur, for example, through interception and inspection of e-mail communications and internet usage records. All employees consent to such monitoring by continuing in their employment after being notified of this computer system policy.

Compliance

Employees are required to notify management upon learning of any violation of this policy. Employees who violate this policy, or who fail to report violations of this policy, will be subject to disciplinary action, up to and including discharge.

Acknowledgment and Consent

All employees are required to sign the following "acknowledgment and consent" form before beginning or continuing active employment. After it is signed it will be kept in the employee's personnel file.

ACKNOWLEDGMENT AND CONSENT

I have received a copy of this {EMPLOYER} computer system policy. I understand that compliance with this policy is a condition of my employment, and that violation of it may result in discipline, up to and including discharge. I also understand that this policy may be revised from time to time in the sole discretion of the company, and that I am required to comply with this policy as revised. I understand that the company may monitor its computer system, and that such monitoring may include but not be limited to interception of and access to my electronic communications, and I voluntarily consent to all such monitoring, with or without prior or subsequent notice. If I have any questions about this policy, or about the appropriate use of the computer system, I will consult my supervisor.

Employee Name (Print): _____

Employee Signature: _____

Date: _____