

Computer Usage Policy

(SAMPLE ONLY. Customize for your needs. Use this sample policy at your own risk. For more information on this or other employment policies we recommend Policies Know by www.knowledgepoint.com)

GENERAL COMPUTING POLICY

THIS AGREEMENT (the "Agreement") is hereby made and entered into by and between [COMPANY] (herein, "Company") and _____ (herein, "You" or "Employee") and entered into on this date: _____. You hereby warrant that you agree and understand that as an Employee, you are responsible for securing the company's network and computing systems against unauthorized access and/or abuse. Any attempt to violate any provision of this policy will result in disciplinary action, up to and including immediate termination. You hereby warrant that you agree and understand that as an Employee you are responsible for obeying all local, state, federal and international laws regarding the use of our computers. Any attempt to break those laws through the use of the Company's computers or network may result in charges and fines being levied against you. In such an event, you hereby agree and understand that the Company will fully cooperate with authorities to provide any information necessary. You further hereby warrant that you agree with and understand the following:

SECTION 1: GENERAL COMPUTING AND OFFICE POLICY

When you receive a user ID to be used to access the network and computer systems on that network, including both our internal network and any external network such as the Internet and commercial online services, you hereby agree and understand that you are solely responsible for all actions taken while using that user ID. And that:

1. Applying for a user ID under false pretenses is a punishable disciplinary offense.
2. Sharing your user ID with any other person is prohibited. In the result that you do share your user ID with another Person, you will be solely responsible for the actions that other person appropriated.
3. Deletion, examination, copying, or modification of files and/or data belonging to other users without their prior consent is prohibited.
4. Use of facilities and/or services for other commercial purposes if prohibited.
5. Use of facilities and/or services for entertainment purposes is prohibited.
6. Use of facilities and/or services for immoral, illegal or unethical purposes if prohibited.
7. Any unauthorized, deliberate action, which damages or disrupts a computing system, alters its normal performance, or causes it to malfunction, is a violation regardless of system location or time duration.
8. Removal of any company property is prohibited.
9. Use of company fax machine, postage machine and copier is for business purposes only.

SECTION 2: GENERAL E-MAIL & VOICE MAIL POLICY

You hereby agree and understand that the Company's e-mail, Internet access, and voice mail systems (which are provided for your use) are for business use only. As such, you hereby agree and understand that the company may monitor both e-mail, Internet access and voice mail systems at will, including the full content of any messages therein, without further disclosure to you. You hereby warrant that you understand that whenever you send electronic mail, your name and user ID are included in each mail message. You are, therefore, responsible for all electronic mail originating from your user ID. Further:

1. Forgery (or attempted forgery) of electronic mail messages is prohibited.
2. Attempts to read, delete, copy, or modify the electronic mail of other users are prohibited.
3. Attempts at sending harassing, obscene and/or other threatening email to another user if prohibited.
4. Attempts at sending unsolicited junk mail, "for-profit" messages or chain letters are prohibited.

SECTION 3: NETWORK SECURITY POLICY

As a user of the network, you may be allowed to access other networks (and/or the computer systems attached to those networks). Therefore:

1. Use of systems and/or networks in attempts to gain unauthorized access to remote systems is prohibited.
2. Use of systems and/or networks to connect to other systems, in evasion of the physical limitations of the remote system/local, is prohibited.
3. Decryption of system or user passwords is prohibited.
4. The copying of system files is prohibited.
5. The copying of copyrighted materials, such as third-party software, without the express written permission of the owner or the proper license, is prohibited.
6. Intentional attempts to "crash" Network systems or programs are punishable disciplinary offenses.
7. The attempts to secure a higher level of privilege on Network systems are punishable disciplinary offenses.
8. The willful introduction of computer "viruses" or other disruptive/destruction programs into the organization network or into external networks is prohibited.

This is a legally binding-Contractual Agreement. Some or all-of the provisions contained herein may survive your employment with The Company. Your signature below indicates that you thoroughly understand and accept these policies as a material condition of your employment and that any violation of any of these provisions may result in severe disciplinary action by the company against you up to and including immediate termination.

AGREED to the date first written above, the parties signed in agreement.
For and behalf of [COMPANY]:

Date:

Employee:
Name (please print):

Date:

Signature:

Prepared by Wayne Higdon, 25th Hour Accounting Solutions, www.25thhour.biz. Revised 10/26/2002. Part of the Accounting Procedures Guide for Nonprofits Using QuickBooks. Contact us for editable copy of this document in MS Word format.