

Note to customer/editor. Please note that this sample policy, as written, is only HRIT's suggestion. You can change or delete any text within our templates.

Use of Electronic Equipment and Resources

The Company provides a variety of electronic equipment and resources to help employees do their jobs efficiently and productively, including telephones, PDAs, voice mail, desktop and portable computers, cell phones, e-mail accounts, internet access, copiers, fax machines, and the like. All such equipment and resources are provided for your use in connection with your job and are the property of the Company.

This policy applies to all equipment and electronic resources that are controlled by the Company, or that are used on or accessed from Company premises, equipment or resources.

Personal Use

Electronic equipment and resources are provided for Company business. However, the Company does permit employees incidental personal use of the computer at their desk or work station during non-working time with their Supervisor's approval. When using a computer for personal use, the employee must not use it in any illegal, obscene, offensive or intimidating manner, or any other manner that violates Company policy. Employees are also prohibited from using company computers or any other resources for personal gain, to compete with the Company in any way, or for the advancement of individual views.

Use of the Company's technical resources must not interfere with your productivity, the productivity of any other employee, or the operation of the Company's technical resources.

Personal use of Company computers is not private. Personal information or messages stored in the Company's systems will be treated no differently from other business-related information and messages, and will be subject to monitoring and review without the employee's prior approval. (See below.)

Confidentiality

All employees have an obligation to safeguard the Company's confidential information, as well as the confidential information of its customer, clients, and others from disclosure. Among other precautions, employees must comply with the following rules:

- a) Always use assigned passwords
- b) Do not access restricted data bases or files without permission
- c) Do not leave any messages containing confidential information visible while you are away from your work area
- d) Always include a statement in e-mail messages containing any confidential or sensitive information, in all capital letters at the top of the message "CONFIDENTIAL - UNAUTHORIZED USE OR DISCLOSURE IS STRICTLY PROHIBITED"
- e) Never store confidential Company information on home computers or laptops without permission and no longer than absolutely necessary for business purposes;
- f) Take all reasonable measures to prevent any portable computer or other equipment containing confidential information from being lost or stolen.

Note to customer/editor. Please note that this sample policy, as written, is only HRIT's suggestion. You can change or delete any text within our templates.

General Use Guidelines

Because of the risk of importing viruses into the Company's computer equipment, employees may not import any hard drives, files or documents that are created outside the Company's premises until the document or file is first scanned for viruses by the computer's anti-virus program.

In addition, only the IT Manager has authority to select software to use on your computer; employees may only install and use software approved by IT. The Company from time-to-time will audit all software on computers in the workplace to identify possible unlicensed, illegal, or unapproved software copies. If such software is found, it will be removed and the person responsible for installing the software, if identified, may be disciplined.

IT or the employee's Supervisor will assign passwords for using Company computers, copiers, e-mail and the Internet. Employees are to use assigned passwords in all appropriate applications. Employees may not share their assigned passwords with anyone, nor may they attempt to guess passwords. All passwords are Company property.

Employees using computers are to make back-up copies of all important documents and files in accordance with the IT Department's back-up protocol system.

Using E-Mail

Because they seem informal, e-mail messages are sometimes offhand, like a conversation, and not as carefully thought out as a letter or memorandum. However, like any other document, an e-mail message can later be used to indicate what an employee said or did.

E-mail messages are also considered to be business records and may be used in investigations by government agencies or private litigation. Some e-mail systems create back-up tapes that make it relatively easy to recover "deleted" e-mail. Consequently, you should not create or send any e-mail that contains any information that you would be embarrassed to have publicized within and outside the Company, or that you would not want to be discovered in a legal proceeding.

Email and attachments can contain viruses that could disable the Company's entire computer network. Exercise extreme caution at all times. Do not open any emails or attachments that look suspicious, even from someone that you know.

Impermissible Uses

Employees must not access, create, store, or transmit intimidating, offensive, hostile or otherwise inappropriate or unprofessional material or communications using any Company-provided electronic resources or equipment or their own personal devices or resources while on Company premises, work-time, or at any time for Company business. The Company's policies against harassment and discrimination apply fully to employees' use of all such equipment and resources, including the e-mail system, voicemail system, mobile phones and Internet access. Any violation of these policies is grounds for discipline up to and including termination of employment.

Employees may not disguise their identity when creating or transmitting messages or material on or from the Company's electronic equipment or resources.

Employees may not open e-mail messages, other than their own or those which the employee is authorized to open by their Supervisor or by the person to whom the e-mail is addressed. Employees may not fake or alter any e-mails, faxes or other communications.

Note to customer/editor. Please note that this sample policy, as written, is only HRIT's suggestion. You can change or delete any text within our templates.

Employees should not copy or distribute copyrighted material (e.g., software, database files, documentation, articles, graphics files, and downloaded information) through the e-mail system or by any other means unless they have confirmed in advance from appropriate sources that the Company has the right to copy or distribute the material. Failure to observe a copyright may result in disciplinary action by the Company as well as legal action by the copyright owner.

Monitoring Employee Use

All Company-provided electronic equipment and resources, and all information transmitted, received or stored in these systems, is the property of the Company. Employees have no right to privacy in their use of Company-provided computers or other electronic equipment and resources, including the Internet, e-mail, instant messaging, text messaging, voicemail, and facsimiles.

The Company reserves the right to randomly monitor and inspect employees' use of its electronic equipment and resources (including e-mail and Internet use, and any information that employees create, store, send or receive), at any time, with or without prior notice to the employee for any legitimate business reason. This includes, but is not limited to, when management has reason to believe the employee may be violating this or any other company policies. **Employees should have no expectation of privacy when using Company-provided equipment or resources.**