Sample Web Acceptable Usage Policy

The Company is pleased to offer associates access to the organization's computer Network and the Internet. This Policy applies to employees granted Network and Internet access by the Company. For the Company to continue making Network and Internet access available, employees must behave appropriately and lawfully. Upon acceptance of your account information and agreement to follow this Policy, you will be granted Network and Internet access in your office. If you have any questions about the provisions of this Policy, you should contact the Chief Information Officer.
If you or anyone you allow to access your account (itself a violation of this Policy) violates this Policy, your access will be denied or withdrawn. In addition, you may be subject to disciplinary action, up to and including termination.

1. Personal Responsibility

By accepting your account password and related information, and accessing the Company's Network or Internet system, you agree to adhere to this Policy. You also agree to report any Network or Internet misuse to the Chief Information Officer. Misuse includes Policy violations that harm another person or another individual's property.

2. Term of Permitted Use

Network and Internet access extends throughout the term of your employment, provided you do not violate the organization's Computer Network and Internet Acceptable Usage Policy. Note: The Company may suspend access at any time for technical reasons, Policy violations, or other concerns.

3. Purpose and Use

The Company offers access to its Network and Internet system for business purposes only. If you are unsure whether an activity constitutes appropriate business use, consult the Chief Information Officer.

4. Netiquette Rules

Employees must adhere to the rules of Network etiquette, or Netiquette. In other words, you must be polite, comply with the Company's ethics policy and code of conduct, adhere to the organization's electronic writing and content guidelines, and use the Network and Internet appropriately and legally. The Company will determine what materials, files, information, software, communications, and other content and activity are permitted or prohibited, as outlined below.

5. Banned Activity

The following activities violate the Company's Computer Network and Internet Acceptable Usage Policy:
(A) Using, transmitting, receiving, or seeking inappropriate, offensive, vulgar, suggestive, obscene, abusive, harassing, belligerent, threatening, defamatory (harming another person's reputation by lies), or misleading language or materials.
(B) Revealing personal information, such as the home address, telephone number, or financial data of another person or yourself.
(C) Making ethnic, sexual-preference, or gender-related slurs or jokes.
(D) Engaging in illegal activities, violating the Employee Handbook, or encouraging others to do so. Examples:
1. Selling or providing substances prohibited by the Company's employment policy or the Employee Handbook.
2. Accessing, transmitting, receiving, or seeking unauthorized, confidential information about clients or colleagues.
3. Conducting unauthorized business.
4. Viewing, transmitting, downloading, or searching for obscene, pornographic, or illegal materials.
5. Accessing others' folders, files, work, networks, or computers. Intercepting communications intended for others.
6. Downloading or transmitting the organization's confidential information or trade secrets.
(E) Causing harm or damaging others' property. Examples:
1. Downloading or transmitting copyrighted materials without permission from the copyright holder. Even when materials on the Network or the Internet are not marked with the copyright symbol, ©, employees should assume all materials are protected under copyright laws—unless explicit permission to use the materials is granted.
2. Using another employee's password to trick recipients into believing someone other than you is communicating or accessing the Network or Internet.
3. Uploading a virus, harmful component, or corrupted data. Vandalizing the Network.
4. Using software that is not licensed or approved by the Company.
(F) Jeopardizing the security of access, the Network, or other Internet Networks by disclosing or sharing passwords and/or impersonating others.
(G) Accessing or attempting to access controversial or offensive materials. Network and Internet access may expose employees to illegal, defamatory, inaccurate, or offensive materials. Employees must avoid these sites. If you know of employees who are visiting offensive or harmful sites, report that use to the Company's Chief Information Officer.
(H) Engaging in commercial activity. Employees may not sell or buy anything over the Internet. Employees may not solicit or advertise the sale of any goods or services. Employees may not divulge private information—including credit card numbers and Social Security numbers—about themselves or others.
(I) Wasting the Company's computer resources. Specifically, do not waste printer toner or paper. Do not send electronic chain letters. Do not send email copies to nonessential readers. Do not send email to group lists unless it is appropriate for everyone on a list to receive the email. Do not send organization-wide emails without your supervisor's permission.
(J) Encouraging associates to view, download, or search for materials, files, information, software, or other offensive, defamatory, misleading, infringing, or illegal content.

6. Confidential Information

Employees may have access to confidential information about the Company, our employees, and clients. With the approval of management, employees may use email to communicate confidential information

internally to those with a need to know. Such email must be marked "Confidential." When in doubt, do not use email to communicate confidential material. When a matter is personal, it may be more appropriate to send a hard copy, place a phone call, or meet in person.

7. Privacy

Network and Internet access is provided as a tool for our organization's business. The computer system is the property of the Company. The Company has the legal right to monitor usage of the Network and the Internet. Employees have no reasonable expectation of privacy when using the Company's computer system, Network, or Internet.

8. Noncompliance

Your use of the Network and the Internet is a privilege, not a right. Violate this policy and, at minimum, your access to the Network and the Internet will be terminated, perhaps for the duration of your tenure with the Company. Policy breaches include violating the above provisions, and failing to report violations by other users. Permitting another person to use your account or password to access the Network or the Internet—including but not limited to someone whose access has been denied or terminated—is a violation of Policy. Should another user violate this Policy while using your account, you will be held responsible, and both of you will be subject to disciplinary action.

Employee Acknowledgment

Note: If you have questions or concerns about this ePolicy, contact the Company's Chief Information Officer before signing this agreement.
I have read the Company's Computer Network and Internet Acceptable Usage Policy and agree to abide by it. I understand violation of any of the above terms may result in discipline, up to and including my termination.

_____ Where's Waldo
Employee Name

_____
Employee Signature

_____
Date