



## **Computer Use and Internet Policy**

This Computer Use and Internet Policy was adopted by Access Health Care Physicians, LLC and Affiliated Companies (collectively, "ACCESS" or the "Company") to assist their Members to fulfill its goal of insuring proper and productive use of computer, network, Internet and telecommunication technology by employees, contractors and other users of ACCESS' computer and telecommunications technologies.

All users of ACCESS' computer and telecommunications technology have the affirmative responsibility for professional, productive, lawful and ethical use of ACCESS' computer resources. Such resources shall be used only for productive goals of ACCESS and not for personal use of the user. Employees and others to which these policies apply may be subject to legal actions, termination, suspension, employment probation, and other potential sanctions, including in some cases possible criminal sanctions, for failure to abide by these policies.

These policies shall be followed when using any of the Company's computer and telecommunication technologies, which shall include, but are not limited to computer work stations, servers (application and mail servers), and internet networks. ACCESS' computer and telecommunication resources include, but are not limited to, the following: host computers, file servers, application servers, mail servers, fax servers and fax machines, communications servers, workstations, laptops, software and internal or external computer and communications networks (including Electronic Data Interchange networks, Internet, newsgroup, commercial online services, bulletin board systems, and e-mail systems) that are accessed directly or indirectly using telecommunication and computer technology owned, leased or otherwise controlled by the Company or used by any party to which these policies apply in furtherance of the Company's goals.

ACCESS may, but is not obligated to, monitor all aspects of its computer and telecommunications technologies. Monitoring activities may include, but are not necessarily limited to monitoring the Internet activity of users. Including websites visited, newsgroups visited, chat group activity, materials that are downloaded or uploaded, reviewing and monitoring e-mails sent and received and monitoring the total time involved in Internet related activities.

Any computer and telecommunications technology used by users and any e-mail and web accounts established by the Company are for use only in furtherance of the job responsibilities and for the betterment of the Company.

Users are placed on notice that they should have no expectation of privacy in their use of ACCESS' computer and telecommunications technologies. All users hereby waive any and all rights to privacy in their usage of the Company's technology and in any item or file that they create access, store, send or receive using the Company's technology. Company representatives are authorized to access, inspect, and review any and all materials that any user creates, stores, accesses, sends, transmits or receives using the Company's technology, and users hereby consent to the same.

All users of ACCESS' computer and telecommunications resources and services shall be subject to the following rules, regulations, policies and standards:

1. Users shall comply with all software licenses and copyrights and with all state, federal and international laws governing intellectual property and online activities. Users shall not be permitted to make any unauthorized copies of software that is resident on any of the Company's technology.
2. Users shall not engage in any fraudulent, harassing, embarrassing, sexually explicit, obscene, intimidation, defamatory or other unlawful or inappropriate material whether through transmission or e-mails, posting in newsgroups, involvement in chat rooms or any other forms of electronic communications. Users encountering or receiving such material or observing or gaining knowledge that others who are subject to these policies may have violated these mandates shall immediately report the incident to their supervisor.
3. No person subject to these policies is authorized to engage in any chat room discussions using ACCESS' technology. No person shall be authorized to place any web pages, postings or other promotional materials promoting the Company of its products or services without the consent of the Company.
4. Without prior written permission of the Company, the computer and telecommunications resources and services of the Company may not be used for the transmission or storage of commercial or personal advertisements, solicitations, promotions, destructive programs (that is, viruses or self-replicating code) political material or any other unauthorized information.
5. Content of all authorized communications should be accurate and concise. Users should use the same care in drafting e-mail and other electronic documents as they would for any other written communication. Anything created on the computer may, and likely will, be reviewed by others.
6. Users are prohibited from sending, receiving, distributing or disclosing any confidential and proprietary information of the Company unless expressly directed to do so by the user's supervisor in furtherance of a valid Company interest.
7. No user is permitted to install software of any kind on the Company's technology. Only software that is placed on the computer technology by the Company IT department shall be authorized. In the event that a user needs additional software that is not provided by the Company, the user shall make a written request to the IT department for such software which written request shall include the bona fide business purpose and function to be accomplished using said software.
8. Any material that is authorized and brought onto the Company's computers or which is authorized and downloaded from the Internet or provided from any other source shall be first scanned for viruses or other destructive elements. Any such items shall be reported to the IT Manager who shall assure that the appropriated virus scanning is performed. Until such virus scanning is performed, even when such item is authorized, it shall not be placed on the Company's computers.
9. Users shall not send unauthorized or unsolicited e-mails to any party. Bulk e-mailing is strictly prohibited.
10. Users shall take all steps necessary to safeguard any password that is assigned for their use. Passwords shall be committed to memory and shall not be auto saved, stored on the computer or network, printed, kept in written form or other hard copy. Users may change their passwords, however, the Company reserves the right to reset any password to allow the Company access to the user's accounts.
11. Users shall comply with all export restrictions applicable to the Company's technology. Specifically, no items including encryptions technology or other restricted technology may

be placed on the internet to otherwise be transmitted, by e-mail or otherwise in any way that could potentially permit access to such materials from outside of the United States.

12. Notwithstanding any term hereof, all users shall be bound by and abide by all other policies, directives and guidelines established by ACCESS, including but not limited to employment policies. All such items shall apply to the user's activities using the Company's technologies.
13. ACCESS is not responsible for material viewed or downloaded by Users from the Internet. Users are cautioned that the Internet is a worldwide network of computers that contains millions of pages of information. Many of these pages include offensive, sexually explicit and inappropriate material. Users accessing the Internet do so at their own risk.
14. Users that think they have received a spam message must forward it to [helpdesk@ahcpllc.com](mailto:helpdesk@ahcpllc.com).
15. Users that think they have clicked a malicious link must report it to [helpdesk@ahcpllc.com](mailto:helpdesk@ahcpllc.com).
16. These policies may be amended and/or restated by the Company at any time. Users shall comply with all such policies and amendments.

The undersigned user executes these policies as a condition of their continuing employment or other relationship with the Company. The user acknowledges that he or she has read and understood these policies and their application to the user. The undersigned agrees to abide by all of the requirements of these policies and understands that failure to abide by these policies may result in sanctions, including but not limited to adverse employment actions, termination of contracts, suspension, employment probation, demotions, termination and potential civil and criminal liability.

---

Applicant Signature

---

Date

---

Applicant Printed Name

Approved as to Form

*Nancy McClain Alfonso*

General Counsel, HCSB