SAM HOUSTON AREA COUNCIL BOY SCOUTS OF AMERICA

Computer Use and Internet Policy

updated August 15, 2003

This document sets the policies of the Sam Houston Area Council Boy Scouts *of* America regarding the use of its e-mail system, Internet system, and communications, which include but are not limited to electronic voice mail, facsimiles, computers and related equipment, the Internet, and the World Wide Web. All employees who use the Sam Houston Area Council network agree to comply with the Council policies as outlined in this policy statement. The Sam Houston Area Council reserves the right to change this policy at any time.

Ownership of Messages. The electronic systems of the Council and all materials created, stored, transmitted, or received using the Council's technical resources are the property of the Council. The Council reserves the right, at all times, and without notice, to review and monitor all such materials whenever, in the Council's discretion, there is a business need to do so. Employees and other users must not create, store, or transmit personal or non-Council business information, messages, or images using Council technical resources.

No Presumption of Privacy. Communications on Council electronic systems are not secure. Employees have no right to privacy with regard to the information, messages, or Images created, stored, transmitted, or received on the Council's system. Passwords and IDs are designed to protect the Council's confidential information from outside third parties, not to provide employees with privacy in their own messages, and other files. In using the Internet and network, employees should be aware that all connections and sites visited could be monitored and traced back to the user. Employees should assume that the communications they create, send, receive, or store might be heard/read by someone other than themselves or the intended recipient.

General Use. Use of council resources and property, including e-mail, Internet access, voice mail, ScoutNET and other technical resources (including the electronic mail (e-mail) system, and Internet access, telephone system, voice-mail system, facsimile machines, copy machines, computer network, modems) are to be used for the Council's business operations.

Message Restriction. Communications on Council electronic systems may not contain content that a reasonable person would consider to be defamatory, offensive, harassing, disruptive, or degrading, including but not limited to offensive language, sexual comments or images, slander, ethnic slurs, or other comments or images that would *offend* someone on the basis of race, sex, national origin, sexual orientation, religion, political beliefs, or disability. Council employees may not use the company's electronic systems in the creation, reception, or distribution of personal messages, communications, chain letters; or distribution of jokes; non-Council purposes; running a personal business venture; or searching for other employment.

Privacy-CD Use-Bandwidth. Employees may not use Council electronic systems to upload or transmit copyrighted, trademarked, patented, confidential, private or proprietary information without proper authorization. Council employees must not use the Internet or Council computers to pirate software, steal passwords, or hack into other machines No unauthorized software may be loaded on to Council systems; this Includes games, screensavers and any program without prior approval. COs may be played on the system but may not be downloaded to the PC hard drive or share drives. The Introduction of viruses, attempts to breach the system, and other malicious tampering with any of the Council electronic systems is expressly prohibited. Connection to live radio uses bandwidth that is intended for Council business and must not be practiced.

Obscene material. Council employees must not use the Internet connection or Council computers to view or exchange pornography or obscene materials. send discriminatory or harassing e-mail, or engage In any other unauthorized activities. Employees may not upload, download, or otherwise transmit any sexually explicit materials or images.

Passwords and Security. No one may allow the use of his/her passwords by others. No one may enable unauthorized third parties to have access to or use of Council systems or otherwise jeopardize the security of the Council's electronic communications systems.

Chats and Auctions, Employees may not participate in newsgroups or chat group sessions unless expressly authorized by the Council. Employees are prohibited from buying and selling personal items on the Council Internet connection.

Conduct and User Responsibility. Employees will be held personally responsible for their conduct on the network or Internet while using Council electronic systems.

Loss and Theft. An employee must reimburse the Council for the full replacement value of any Council-owned equipment (including, but not limited to, notebook computers, desktop computers, cell phones, personal digital assistants, software, and projectors) that is lost or stolen while in the employee's possession while away from Council property. Employees must store notebook computers in a locked and secure place at the end of the business day. If the employee prefers, she/he may take the notebook computer home. (A Council laptop must never be left in an unattended automobile, truck or public place. When an employee travels and must leave her/his car parked in a public place, the laptop must be placed in the trunk of the employee's car to help prevent theft. Once home, the employee must place the laptop in a temperature regulated room.)

Connection to the Council Network. Employees who connect to the Council network with computers they personally own must receive written approval from the Information Systems Director of IT Infrastructure for ail programs and applications that are downloaded to those computers. Employee-owned computers. that are connected to the Council Network MUST NOT contain tile-sharing applications like AOL Instant Messaging (AIM), Microsoft's Instant Messenger, KaZaa, and other unapproved applications. Periodic and unannounced audits will be conducted on all computers that connect to the Council's Network. Employees unwilling to follow these guidelines will not be permitted to connect to the Council's Network.

Sanctions. Violations of the policies described above for legal and ethical use of computing resources will be dealt with seriously. Violators will be subject to the normal disciplinary procedures of the Council, which may include dismissal. lllegal acts involving the Sam Houston Area Council's computing resources may also be subject to prosecution by local, state and federal authorities.

I have read and agree to abide by this policy in regards to the use of Council owned and or supported electronic systems provided by the Council.

Name: _____ Signature: _____ Date: _____

Parent/Guardian (if minor): _____ Signature: _____ Date: _____

Name: _____