INTERNET, E-MAIL & ELECTRONIC RESOURCES POLICY

POLICY STATEMENT ON USE OF TOA ELECTRONIC RESOURCES

The use of Texas Orthopaedic Association ("TOA") electronic resources, including computers, fax machines, telephone systems, company issued cell phones (including text messages therefrom), and all forms of e-mail and Internet/intranet access, is for TOA business and for authorized purposes only. Brief and occasional personal use of electronic resources, including e-mail and the Internet is acceptable as long as it is not excessive or inappropriate, occurs only during personal/nonworking time (lunch or other breaks), and does not result in expense or harm to TOA or otherwise violate this policy.

UNACCEPTABLE USE OF ELECTRONIC RESOURCES

Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities. Electronic communication should not be used to solicit or sell products or services that are unrelated to TOA's business; distract, intimidate, or harass coworkers or third parties; or disrupt the workplace.

Use of TOA electronic resources, including computers, networks, and Internet access is a privilege granted by management and may be revoked at any time for inappropriate conduct carried out on such systems and lead to discipline. Examples of unacceptable uses of electronic resources include, but are not limited to:

- Excessive use of personal e-mail or the Internet;
- Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam") that is unrelated to legitimate TOA purposes;
- Engaging in private or personal business activities, including excessive use of instant messaging and chat rooms (see below);
- Accessing networks, servers, drives, folders, or files to which the employee has not been granted access or authorization from someone with the right to make such a grant;
- Making unauthorized copies of TOA files or other TOA data;
- Destroying, deleting, erasing, or concealing TOA files or other TOA data, or otherwise making such files or data unavailable or inaccessible to TOA or to other authorized users of TOA systems;
- Misrepresenting oneself or TOA
- Violating the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way;
- Engaging in unlawful or malicious activities;
- Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either TOA's networks or systems or those of any other individual or entity;
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;
- Sending, receiving, or accessing pornographic materials;
- Becoming involved in partisan politics;
- Causing congestion, disruption, disablement, alteration, or impairment of TOA networks or systems;

- Maintaining, organizing, or participating in non-work-related Web logs ("blogs"), Web journals, "chat rooms", or private/personal/instant messaging;
- Failing to log off any secure, controlled-access computer or other form of electronic data system to which you are assigned, if you leave such computer or system unattended;
- Using recreational games; and/or
- Defeating or attempting to defeat security restrictions on company systems and applications.

Using TOA automation systems to access, create, view, transmit, or receive racist, sexist, threatening, or otherwise objectionable or illegal material, defined as any visual, textual, or auditory entity, file, or data, is strictly prohibited. Such material violates TOA's anti-harassment policies and is subject to disciplinary action. TOA's electronic mail system, Internet access, and computer systems must not be used to harm others or to violate the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way. Use of company resources for illegal activity will lead to disciplinary action, up to and including dismissal and criminal prosecution. TOA will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual Internet activities, e-mail use, and/or computer use.

Employees are prohibited from installing any software on company computers. This policy will ensure that TOA can manage the software on company systems, prevent the introduction of computer viruses, and meet its obligations under applicable software licenses and copyright laws. TDS reserves the right at any time to inspect and screen its electronic resources. If any outside applications or software are discovered, they will be removed immediately. Violators are subject to discipline, up to and including termination of employment.

Employees may not utilize TOA electronic resources, including but not limited to cell phones and blackberries, while operating a motor vehicle or other motorized equipment/vehicles unless the employee is utilizing a hands-free device such as a bluetooth.

TOA telephone system (including TOA issued cell phones) is intended for the conduct of TOA business. Although employees may utilize the telephone system for occasional personal calls, discretion should be used. Personal telephone calls during work hours are discouraged. Excessive personal use is prohibited and will lead to discipline.

Unless specifically granted in this policy, any non-business use of TOA's electronic resources is expressly forbidden.

If you violate these policies, you could be subject to disciplinary action, up to and including dismissal.

OWNERSHIP AND ACCESS OF ELECTRONIC RESOURCES; NO EXPECTATION OF PRIVACY

TOA owns the rights to all data and files in any computer, network, or other information system used in TOA and to all data and files sent or received using any company system or using TOA's access to any computer network. **TOA monitors the use of all TOA electronic resources, including electronic mail messages (including personal/private/instant messaging systems) and their content, as well as any and all use by employees of the Internet and of computer equipment used to create, view, or access e-mail and Internet content, and all telephone calls from TOA phone lines (including TOA issued cell phones).** Employees must be aware that the electronic mail messages sent and received using TOA equipment or TOA-provided Internet access, including web-based messaging systems used with such systems or access, are not private and are subject to viewing, downloading, inspection, release, and archiving by TOA officials at all times. TOA has the right to inspect any and all files stored in private areas of the network or on individual computers or storage media in order to assure compliance with TOA policies and state and federal laws. No employee may access another employee's computer, computer files, or electronic mail messages without prior authorization from either the employee or an appropriate TOA official.

Employees have no expectation of privacy while using TOA electronic resources. TOA uses software in its electronic information systems that allows monitoring by authorized personnel and that creates and stores copies of any messages, files, or other information that is entered into, received by, sent, or viewed on such systems. Accordingly, employees should understand that whatever they do, type, enter, send, receive, and view on TOA electronic information systems is electronically stored and monitored. Further, employees who use TOA electronic systems and Internet access to send or receive files or other data that would otherwise be subject to any kind of confidentiality or disclosure privilege thereby waive whatever right they may have to assert such confidentiality or privilege from disclosure. Employees who wish to maintain their right to confidentiality or a disclosure privilege must send or receive such information using some means other than TOA systems or TOA-provided Internet access.

CONFIDENTIALITY OF ELECTRONIC MAIL

As noted above, electronic mail is subject at all times to monitoring, and the release of specific information is subject to applicable state and federal. Existing rules, policies, and procedures governing the sharing of confidential information also apply to the sharing of information via commercial software. Since there is the possibility that any message could be shared with or without your permission or knowledge, the best rule to follow in the use of electronic mail for non-work-related information is to decide if you would post the information on the office bulletin board with your signature.

ELECTRONIC MAIL TAMPERING

Electronic mail messages received should not be altered without the sender's permission; nor should electronic mail be altered and forwarded to another user and/or unauthorized attachments be placed on another's electronic mail message.

INTERNET USE

The Internet is to be used to further TOA's business, to provide effective service of the highest quality to TOA's customers and staff, and to support other direct job-related purposes. Supervisors should work with employees to determine the appropriateness of using the Internet for professional activities and career development. The various modes of Internet access are TOA resources and are provided as business tools to employees who may use them for research, professional development, and work-related communications.

Limited personal use of the Internet is permissible during personal/nonworking time and is subject to the restrictions noted herein.

Employees are individually liable for any and all damages incurred as a result of violating company security policy, copyright, and licensing agreements.

All TOA policies and procedures apply to employees' conduct on the Internet, especially, but not exclusively, relating to: intellectual property, confidentiality, company information dissemination, standards of conduct, misuse of company resources, anti-harassment, and information and data security.

STATEMENT ON TEXT MESSAGING

Text messages sent via TOA cell phones or electronic devices are subject to the terms of this Policy. Employees are cautioned that excessive text messaging from personal phones during working hours is prohibited, as is sending or receiving any text message which would violate any other TOA policy, including its anti-harassment policy. Sending or receiving text messages while driving any TOA vehicle is strictly prohibited.

PERSONAL ELECTRONIC EQUIPMENT

TOA prohibits the use or possession in the workplace of any type of camera phone, cell phone camera, digital camera, video camera, or other form of image- or voice-recording device without the express permission of TOA and of each person whose image and/or voice is/are recorded. Employees with such devices should leave them at home unless expressly permitted by TOA to do otherwise. This provision does not apply to designated TOA personnel who must use such devices in connection with their positions of employment.

Employees should not bring personal computers or data storage devices (such as floppy disks, CDs/DVDs, external hard drives, flash drives, iPods, or other data storage media) to the workplace or connect them to TOA electronic systems unless expressly permitted to do so by TOA. Any employee bringing a personal computing device, data storage device, or image-recording device onto TOA premises thereby gives permission to TOA to inspect the personal computer, data storage device, or image-recording device at any time with personnel of TOA's choosing and to analyze any files, other data, or data storage devices or media that may be within or connectable to the personal computer or image-recording device in question. Employees who do not wish such inspections to be done on their personal computers, data storage devices, or imaging devices should not bring such items to work at all.

Violation of this policy, or failure to permit an inspection of any device covered by this policy, shall result in disciplinary action, up to and possibly including immediate termination of employment, depending upon the severity and repeat nature of the offense. In addition, the employee may face both civil and criminal liability from TOA, from law enforcement officials, or from individuals whose rights are harmed by the violation.