Acceptable Use Policy

Version Number: 1.0

Notices

This document was written and produced by:

American Academy of Orthopaedic Surgeons
9400 West Higgins Road
Rosemont, Illinois 60018-4976

Table of Contents

Revision Log

Date	Author	Modifications	Document Version
10/26/2018	Risk Management Team	Policy Adopted	1.0

1 Introduction

The use of technology resources is critical to the American Academy of Orthopaedic Surgeons' (AAOS) mission. Although technology resources promise faster and better communications, they also raise significant issues concerning the security, privacy and control of information.

2 Purpose

This policy accordingly defines the parameters of appropriate and professional use of AAOS's technology resources.

3 Scope

This policy applies to (1) all American Academy of Orthopaedic Surgeons ("AAOS") employees including employees authorized to work from home and all other persons authorized to use AAOS technology resources, including contractors, vendors and other third parties (collectively "users"); (2) all AAOS technology resources, including but not limited to computers, mobile devices (such as cell phones and personal tablet devices), servers, networks, printers and any other computer peripheral, software, data storage media, e-mail, telephones, voice mail, fax machines, photocopiers, internet and intranet access (collectively, "technology resources"); and (3) all data created, entered, received, stored, accessed, viewed or transmitted using AAOS technology resources, including but not limited to all communications, work products, and all information maintained or owned by AAOS.

4 Right to Modify Policy

The American Academy of Orthopaedic Surgeons reserves the right to modify this Acceptable Use Policy at any time. Changes and modifications will be effective when approved and posted.

5 Definitions

Confidential Data is information that is not available to the general public and is personally identifiable information that is considered private in nature, such as health information, addresses, prior work experience, and financial data.

Due Care is the degree of care that an ordinary and reasonable person would normally exercise, over his or her own property or under circumstances like those at issue.

Jailbroken (or **Rooted**) To jailbreak/root a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software.

Mobile Devices is a small computing device, typically small enough to be handheld. Mobile devices have a display screen with touch input and/or a miniature keyboard. A handheld computing device has an operating system (OS), and may run various types of application software, known as apps. Most handheld devices may also be equipped with Wi-Fi, Bluetooth, NFC and GPS capabilities that may allow connections to the Internet and other devices, such as an automobile or a microphone headset or may be used to provide location-based services.

Rooted *see* ***Jailbroken***

Sensitive Data is information that must be protected from unauthorized access to safeguard the privacy or security of an individual or organization.

TDS (Technology & Data Services) is the AAOS department responsible for maintaining and securing organizational technology and data resources.

Tethering is connecting one device to another. In the context of mobile phones and tablet computers, tethering allows sharing the Internet connection of the phone or tablet with other devices such as laptops or vice versa. Connection of the phone or tablet with other devices may be done over Bluetooth or by physical connection using a cable, for example through USB.

6 Policy

6.1 Proper Use

Other than occasional personal use of voice mail, e-mail and Internet access, AAOS-provided technology resources may be used only for legitimate AAOS business related purposes. Occasional personal use means infrequent, incidental use that is professional, does not interfere with the user's working time or the working time of another user, does not strain the availability, usability, or costs of AAOS's technology resources, and that does not violate this or other AAOS policies. All use of AAOS technology resources -- including all personal use -- is subject to this policy. This policy should not be construed to interfere with any rights protected under federal, state or local law.

6.2 Data Ownership

All information and data created, entered, received, stored, accessed, viewed or transmitted via AAOS technology resources is AAOS property. The AAOS has a perpetual, royalty-free, irrevocable, non-exclusive right and license to use, reproduce, modify, adapt, publish, distribute and incorporate all such data, except that the AAOS will not publicly disclose or use non-AAOS information received from third parties or certain confidential information without proper authorization.

6.3 Data Classification

AAOS employees and contractors must take reasonable precaution to secure AAOS intellectual property, including data and data entrusted to AAOS from unauthorized use or disclosure. For these purposes, all data or information produced and shared within or parties outside the organization should be properly classified and labeled appropriately.

For Protected Information, use the label ***AAOS PROTECTED***. This contains information protected by federal and/or state laws and regulations. Any further use or disclosure of this information is strictly prohibited, unless written authorized is obtained.

For Confidential Information, use the label ***AAOS CONFIDENTIAL***.

For Internal Use Only, use the label ***AAOS INTERNAL USE ONLY***.

For additional clarification of where and when to apply this classification level, refer to the AAOS Corporate Security Policy Data Classification section or contact the AAOS Data Privacy Officer or Information Security Officer.

6.4 Monitoring

As with all other AAOS property, AAOS will search, monitor, inspect, intercept, review, access and/or disclose all AAOS technology resources and all data created, entered, received, stored, viewed, accessed or transmitted via those resources for any reason, at any time, and without notice based on business need or legal requirements. For example, authorized persons will inspect the AAOS's technology resources to respond to legal investigations, investigate theft, the unauthorized disclosure of proprietary information, misuse, and to assess Internet use or use of any other technology resource. The AAOS will attempt to ensure that monitoring and inspections are conducted professionally. In this regard, no employee may monitor or intercept any data without the approval of the TDS Department and authorization from AAOS's Legal and/or Human Resources Departments, or persons designated by them or acting at their direction.

6.5 No Privacy

Users should have no expectation of privacy about the use of any aspect of AAOS technology resources, including the creation, entry, receipt, storage, accessing, viewing or transmission of data or information.

6.6 Passwords and Data Security

All passwords and security used to access AAOS technology resources, including voice mail access codes are AAOS property. Users must understand that their use of passwords will not preclude access, monitoring, inspection, review, or disclosure by authorized AAOS personnel. The AAOS TDS Department also may unilaterally assign, audit, and/or change passwords and other codes that access AAOS technology resources.

The security of the AAOS's technology resources is every user's responsibility. Passwords must be maintained as confidential and shall not be shared with other users or third parties. Generic or shared logins and passwords approved for use by TDS are the only exceptions. Passwords may not be placed in areas where they may be discovered (such as on post it notes near computers). Accidental disclosure of a password, or a password that is suspected of being lost, stolen, or compromised should be reported immediately to the user's supervisor and TDS, and the user or the Technology Department shall immediately change the password. Individual passwords are required to be changed on a reoccurring basis as specified by TDS.

If any information and or data that is lost, exfiltrated, or disclosed to unauthorized parties, or suspected of being lost, exfiltrated or disclosed to unauthorized parties, the appropriate department head from which the information was lost, and the Chief Information Office or Information Security Officer must be notified immediately. Users must immediately notify the Chief Human Resources Officer of any violations of this policy.

6.7 Unauthorized Access

Unauthorized access of AAOS technology resources and/or disclosure of other users' passwords is strictly prohibited. For example, users are prohibited from accessing other users' files or communications without the express permission of that user or the permission of AAOS's Legal and/or Human Resources Departments, or persons designated by them or acting at their direction.

In addition, data within AAOS technology resources are to be accessed only by users with a legitimate business purpose for accessing the information. For example, "browsing" through AAOS data or files without a legitimate business reason is prohibited.

6.8 Appropriate and Lawful Use

Users are forbidden from using AAOS technology resources in any way that may be construed to violate the AAOS's harassment-free workplace policy or other workplace policies. This prohibition includes sexually explicit or offensive images, messages, cartoons, jokes, ethnic or religious slurs, racial epithets or any other statement or image that might be construed as harassment or disparagement based on race, color, religion, sex, national origin, age, disability, sexual orientation, or any other status protected by law. Users are required to take all reasonable steps to avoid and eliminate receipt from known sources of all potentially offensive material.

AAOS technology resources may not be used to intentionally or unintentionally violate any local, state, federal or international civil or criminal law, including copyright (through, for example, the uploading or downloading of copyrighted content such as music, videos or software) and patent laws and/or U.S. Securities and Exchange Commission

regulations. Unlawful activity includes but is not limited to lotteries, raffles, betting, gambling for anything of value (e.g., Final Four tournaments, "fantasy football") and participating or facilitating in the distribution of unlawful materials. Users also may not upload, post, e-mail or otherwise transmit any data that is threatening, malicious, tortious, defamatory, libelous, obscene, or invasive of another's privacy. In addition, AAOS technology resources may not be used to run or solicit outside business ventures.

6.9 Confidential Information and use of Intellectual Property

Users may not place, post, transmit or otherwise disclose confidential, sensitive and/or proprietary client or AAOS information or confidential user information (such as social security numbers, personally identifiable data) to anyone outside of the AAOS by any means, at any time or for any reason without authorization from the Legal and/or Human Resources Departments. Refer to the AAOS Security Policy for additional details related to data security and compliance requirements.

AAOS's name, trademarks, service marks, logos or other intellectual property (including AAOS data) may not be used outside the scope of a user's assigned employment duties without the express authorization of the appropriate Department Head.

6.10 Misrepresentation of Identity and/or Data

AAOS technology resources may not be used to misrepresent, obscure, suppress, or replace one's identity or the origin of data or communications. For example, "spoofing" (i.e., constructing electronic communications to appear to be from somebody else) is prohibited. Each user's name, e-mail address, organizational affiliation, time and date of transmission, and related information included with electronic communications (including postings) must always reflect the true originator, time, date, and place of origination, as well as the original message's true content.

6.11 Spam, Chain Letters and Games

AAOS technology resources may not be used to transmit junk mail, chain letters, mass personal or commercial solicitations, or spam (the same or substantially similar messages sent to many recipients for commercial or other purposes unrelated to the AAOS). Users may not participate or conduct pyramid schemes of any kind and may not download or execute games.

6.12 Viruses/Malware

Users may not intentionally upload, post, e-mail or otherwise transmit any material that contains software viruses, malware, or any other malicious computer code, files or programs designed to interrupt, destroy, or limit the functionality of any computer software, hardware or telecommunications equipment. The AAOS maintains and uses virus, spyware, and malware prevention software. Aiding in the prevention of computer viruses from compromising AAOS technology resources is the responsibility of all users.

Consistent with this Policy, users are prohibited from disabling or bypassing the AAOS's virus detection/prevention software, using unauthorized hardware or software, or downloading files or software from the Internet that is inconsistent with legitimate AAOS business purposes.

6.13 Software, Cloud (e.g. SaaS, PaaS, IaaS), and Hardware Installation

No software or hardware of any kind shall be installed on any AAOS technology resources (including desktop, laptop or server computers) without prior approval by TDS. This includes, by way of example only, unauthorized data storage devices, "plug in" and "helper" applications, games, screensavers, desktop wallpaper, ActiveX Controls, Outlook add-ins, etc.

The use of third-party applications and services for business purposes without the prior approval by TDS is strictly prohibited. TDS must review and approve the use of all third-party cloud agreements prior to committing to contracts or subscription services. Only approved Cloud services authorized by TDS shall be utilized by AAOS technology resources and employees. All unapproved Cloud services shall be deemed unauthorized and are not reimbursable by AAOS.

6.14 Software Licensing Compliance

The AAOS performs internal software audits on a frequent basis. The audit process ensures that the AAOS maintains software licensing compliance as agreed to in our software license agreements. Software licenses remain the property of the AAOS and may be reclaimed from a user at any time. Unlicensed, illegal, or pirated software may not be installed on AAOS technology resources.

6.15 Hardware

TDS establishes the standards for technology resources such as computer hardware acquisitions, including the standards related to the lease, purchase or rental of hardware; the brand of hardware and peripheral equipment; maintenance contracts; and service vendors. Unless authorized by TDS, while on AAOS premises, users may not use personal computing hardware/devices to either modify their computer workstations or access the AAOS network.

6.16 E-Mail and Data Storage

All E-Mail and Data created, entered, received, stored, accessed, viewed or transmitted via AAOS technology resources is AAOS property.

All AAOS Email must be stored on AAOS email server systems. The use of any other unauthorized email service for business purposes is prohibited. This includes the use of personal email services such as Gmail or individual email archives (also known as "PST files," "Personal Folders" or "Personal Archives"). AAOS data must not be stored on a

user's local hard drive of their computer. To ensure that data is kept secure and that disaster recovery backups of AAOS data are performed, the AAOS requires all business data be stored within departmental shared network folders or within AAOS provided personal network storage locations on AAOS file servers or AAOS managed services. The use of portable removable storage devices (such as flash drives, external hard drives, smart phones with local storage, etc.) and personal cloud storage services such as Google Drive, Dropbox or similar is prohibited unless authorized by TDS management. All such portable or cloud data storage devices and services must be procured through the Technology Department by submitting a Technical Support ticket stating the business requirement for such a device. Users are not permitted to connect personal data storage devices to AAOS technology resources.

6.17 Mobile Devices

AAOS recognizes that mobile devices are useful tools in enabling productivity. Mobile devices may help employees maintain a single up-to-date calendar, check e-mails, take notes during meetings and support other work-related activities. This Mobile Device Policy declares what is acceptable with regards to utilizing mobile devices at AAOS, it encompasses both privately owned and AAOS provided mobile devices. This policy serves as a framework for the AAOS organization to implement the Mobile Device Procedure.

AAOS grants its employees the privilege of purchasing and using smartphones and tablets of their choosing at work for their convenience. AAOS reserves the right to revoke this privilege if users do not abide by the policies and procedures as outlined.

This policy is intended to protect the security and integrity of AAOS's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms and will be approved and documented by TDS support.

AAOS employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the AAOS internal corporate network and services such as email and file storage locations.

6.17.1 Mobile Device Acceptable Use Requirements

The following must be accepted by the employee requesting access to AAOS resources via a mobile device prior to approval:

- The employee agrees and is expected to use his or her mobile device in an ethical manner at all times and adhere to the company's acceptable use policy as outlined herein.
- Requests to connect to the messaging network or other AAOS resources from a mobile device will be quarantined until approved by TDS.
- AAOS provided mobile devices or tablets will remain the property of AAOS for the duration of their useful life and returned to AAOS if the approved employee's employment ends.

- Users may only access and view AAOS data that is essential to their job role on their mobile device(s).
- Employee's will be restricted to no more than 3 mobile devices approved and active for use at any given time to access AAOS resources.
- Employees may use their mobile device to access the following company-owned resources: MS Exchange (email, calendars, contacts); AAOS approved Office365 apps; or other similar resources as determined by AAOS in compliance with policy.
- AAOS has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.
- Users must report all lost or stolen devices to the TDS support desk within a 24-hour time frame. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- If a user suspects that unauthorized access to AAOS data has taken place via a mobile device, they must report the incident to TDS by contacting the support desk.
- Mobile devices must not be "jailbroken" or "rooted" or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the end user.
- Mobile device users must not load pirated software or illegal content onto their devices. This includes P2P streaming services and anonymized software applications.
- Mobile software applications must only be downloaded and installed from approved sources. This includes the official software publisher's website or directly from the trusted app store (for example, Apple's App Store) available for the mobile device's operating system.
- Mobile Devices must be kept up to date with manufacturer or network provided patches or latest mobile operating system version. At a minimum, employee shall check monthly and apply the update as soon as possible.
- Mobile Devices must not be connected via Bluetooth, USB or Tethering to any PC which does not have up to date and enabled anti-malware protection.
- Mobile Devices must be encrypted and in alignment with AAOS's data protection standard as outlined in the Corporate Security Policy.
- Users must be cautious about the merging of personal and work email accounts on their devices. They must practice Due Care to ensure that AAOS data is only sent through the corporate email system via a native Microsoft Exchange supported application or the AAOS Mimecast Mobile Application.
- Employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

- The end user is responsible for the backup of their own personal data. AAOS will accept no responsibility for the loss of files due to a non-compliant device being wiped for security reasons.
- Users must not use AAOS provided workstations to backup or synchronize device content such as media files, unless such content is required for legitimate business purposes.
- AAOS reserves the right to disconnect devices or disable services without notification.

6.17.2 Devices and Support

- Smartphones including iPhone, Android and Windows phones are allowed and must be running an approved, native and commercially available mobile device operating system for that device which is no more than two versions behind the latest production release.
- Tablets including iPad and Android are allowed and must be running a native commercial device mobile operating system that is no more than two versions behind the latest production release.
- TDS support will make best effort attempts to resolve any connectivity issues with personal devices. Employees should contact their device manufacturer or wireless provider for operating system or hardware-related issues.
- While TDS will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.

6.17.3 Reimbursement

Refer to the AAOS Employee Manual or contact Human Resources for information related to employee device reimbursement policy.

6.17.4 Mobile Device Network Traffic Monitoring

AAOS will proactively monitor the network traffic to and from mobile devices. AAOS has configured certificate-based access to corporate applications, email, VPN and Wi-Fi networks. Incoming network traffic will be filtered by IP address or protocol.

Monitoring will be performed in accordance with the AAOS Corporate Security Policy. Any device that fails to meet the minimum standards defined by AAOS policy will be proactively removed from the organizational network.

The following will be monitored at AAOS:

- **Anomalous behavior.** This will include observing the activities of mobile users, devices and processes, and measuring these activities against a baseline of unknown normal activity to detect abnormal behavior.

- **Device compliance.** Monitoring devices to ensure they remain compliant with the AAOS mandated set of policies for mobile devices including use of passwords, phone locks and remote wipe capability.
- **Rooting and jailbreaks.** Detection will be implemented to ensure that the security architecture for mobile devices has not been compromised by rooting or jailbreaking devices (the process of subverting the system).
- **Geo-fencing.** A device's location will be monitored and where appropriate network resources will allowed/disallowed based on that location. The AAOS network will be subject to continuous scan/asset discovery process to discover all mobile devices, including unauthorized assets.
- **Mobile device inventory** including its applications and users will be logged by AAOS.
- **Ongoing application risk***.* Mobile device applications will be monitored and any that are deemed to be subsequently assessed as high risk to the organization will be denied access to organizational resources until full compliance is met.

6.18 Utilization of Cloud based applications and AAOS Data

AAOS supports the use of the following cloud storage solutions for use by AAOS staff and approved contract resources:

- OneDrive (AAOS domain credentials only)
- SharePoint Online (AAOS domain credentials only)
- Mimecast (AAOS domain credentials only)

AAOS Non-Sanctioned Cloud storage solutions: AAOS does not support the use of non-sanctioned cloud storage solutions. Use non-sanctioned cloud storage solutions for storage of AAOS business data (permanent or temporary) without prior written approval by TDS Management is prohibited. Below is a partial list for example.

- OneDrive with (Personal E-mail Account)
- Dropbox
- Google Drive
- Mega
- iCloud
- Box
- NextCloud
- Amazon Drive

6.19 Removal of Technology Resources

AAOS issued technology resources may only be removed from AAOS premises by a user who has received proper authorization to do so from both their appropriate Department Manager and TDS. TDS issued notebook or laptop computers for business use are the only exception.

6.20 Third Party Use

Only authorized users may operate AAOS technology resources. No user may grant or permit any third party (including customers and suppliers, family or friends) to access any technology resourced without prior approval of both their appropriate Department Manager and TDS.

6.21 Terminated at Separation

Before each user's last day of employment, he or she shall return or otherwise surrender possession to all AAOS technology resources (including computers, mobile devices, software programs, computer peripherals, electronically stored data, data storage devices, keys, and written passwords) in his or her possession, custody or control. Upon separation of employment, the AAOS will terminate user access to AAOS technology resources.

Notice of user terminations must be provided to Human Resources in accordance with AAOS policy. Managers are responsible for retrieving all technology resourced from terminated users and notifying the TDS.

6.22 Exceptions

Any exception to this Policy must be approved in writing by the AAOS Human Resources Department, General Counsel and the Chief Information Officer.

6.23 Policy Violations

Access to and use of AAOS technology resources is a privilege, not a right. Users who do not comply with this policy are subject to denial of access to AAOS technology resources and disciplinary action up to and including termination.

6.24 Revisions

The AAOS may amend, revise or depart from this policy at any time, with or without notice. This policy does not constitute and shall not be construed as an express or implied contract of employment. Because technology is constantly changing and evolving, all users are expected to periodically review and familiarize themselves with this policy and with any subsequent updates to this policy.

