American Pediatric Surgical Nurses Association Inc. *Safety and Excellence in the Surgical Care of Children*	POLICY AND PROCEDURE
PAGE: 1 of 6	**REPLACES POLICY DATED: April 1, 2017**
EFFECTIVE DATE: April 12, 2020	**APPROVED BY:** APSNA BOD 2022-2023
NEXT REVISION: April, 2026	
POLICY DESCRIPTION: Information Technology (IT) Resources and Communication Systems Policy	
REVIEWED: 4/23	**REVISION: 4/20**

The American Pediatric Surgical Nurses Association, Inc. ("APSNA")'s computers, networks, communications systems and other IT resources are intended for business purposes only (except for limited personal use as described below) during working time and at all other times. To protect APSNA and its board members, officers and members, it is the organization's policy to restrict the use of all IT resources and communications systems as described below. Each user is responsible for using these resources and systems in a productive, ethical and lawful manner.

The organization's policies prohibiting harassment, namely Conflict of Interest Policy, Copyright Guidelines Policy, Document Retention Policy, Non-Discrimination Harassment Policy, Social Media, Statement of Values and Ethical Standards, Diversity, Bullying and Incivility apply to the use of the organization's IT resources and communications systems. No one may use any communications or computer system in a manner that may be construed by others as harassing or offensive based on race, national origin, sex, sexual orientation, age, disability, religious beliefs or any other characteristic protected by federal, state or local law.

The use of APSNA's IT resources and communications systems by a member shall signify his or her understanding of and agreement to the terms and conditions of this policy, as a condition of membership.

Administration of this Policy.

The Secretary is responsible for the administration of this policy. If you have any questions regarding this policy, please contact the Secretary at info@apsna.org.

In the event that any action by APSNA is necessary in respect to this policy, the Board of Directors may delegate sufficient authority to one or more members of the board of directors of APSNA to carry out such actions.

Security, Access and Passwords.

Security of APSNA's IT resources and communications systems is the responsibility of the Secretary and Web Administrator, including approval and control of members' and others' access to systems and suspension or termination of access in cases of misuse and when a user is no longer a member or otherwise ineligible to use the systems.

It is the responsibility of each member to adhere to IT security guidelines including but not limited to the creation, format and scheduled changes of passwords. All usernames, pass codes, passwords, and information used or stored on the organization's computers, networks and systems are the property of APSNA. No member may use a username, pass code, password or method of encryption that has not been issued to that member or authorized in advance by the organization.

No member shall share usernames, pass codes or passwords with any other person except as otherwise expressly authorized in writing by APSNA. A member shall immediately inform the Secretary at info@apsna.org if he/she knows or suspects that any username, pass code or password has been improperly shared or used, or that IT security has been violated in any way.

Resources and Systems Covered by This Policy. This policy governs all IT resources and communications systems owned by or available at APSNA, and all use of such resources and systems when accessed using a member's own resources, including but not limited to:

- Email systems and accounts including file sharing and document archives.
- Internet and intranet access.
- Telephones and voicemail systems, including wired and mobile phones, smartphones and pagers.
- Printers, photocopiers and scanners.
- Fax machines, e-fax systems and modems.
- All other associated computer, network and communications systems, hardware, peripherals and software, including network key fobs and other devices.
- Closed-circuit television (CCTV) and all other physical security systems and devices, including access key cards and fobs.

No Expectation of Privacy. All contents of APSNA's IT resources and communications systems are the property of the organization. Therefore, members should have no expectation of privacy whatsoever in any message, files, data, document, facsimile, telephone conversation, social media post, conversation or message, or any other kind or form of information or communication transmitted to, received or printed from, or stored or recorded on the organization's electronic information and communications systems.

You are expressly advised that in order to prevent against misuse, **APSNA reserves the right to monitor, intercept and review, without further notice, every member's activities using the organization's IT resources and communications systems, including but not limited to email (both outgoing and incoming), telephone conversations and voice mail recordings, instant messages and internet and social media postings and activities, and you consent to such monitoring by your acknowledgement of this policy and your use of such resources and systems.** This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

The organization may also store copies of such data and communications for a period of time after they are created and may delete such copies from time to time without notice.

Do not use the organization's IT resources and communications systems for any matter that you desire to be kept private or confidential from the organization.

Confidentiality and Proprietary Rights

APSNA's confidential information and intellectual property (including trade secrets) are extremely valuable to APSNA. Treat them accordingly and do not jeopardize them through your business or personal use of electronic communications systems, including email, text messaging, internet access, social media and telephone conversations and voice mail.

Do not use APSNA's name, brand names, logos, taglines, slogans or other trademarks without written permission from the Secretary at info@apsna.org.

This policy also prohibits use of the organization's IT resources and communications systems in any manner that would infringe or violate the proprietary rights of third parties. Electronic communications systems provide easy access to vast amounts of information, including material that is protected by

copyright, trademark, patent, and/or trade secret law. You should not knowingly use or distribute any such material downloaded from the internet or received by email without the prior written permission of the Secretary.

Email and Text Messaging.

APSNA provides certain members with access to email systems for use in connection with the performance of their duties. APSNA seeks to provide stable and secure email systems (including SMS and internet-based instant messaging) with rapid, consistent delivery times that promote communication for business purposes without incurring unnecessary costs or generating messages that are unproductive for the recipient. Many of the policies described below governing use of the organization's email systems are aimed at reducing the overall volume of messages flowing through and stored on the network, reducing the size of individual messages, and making the system more efficient and secure.

Spam. Unfortunately, users of email will occasionally receive unsolicited commercial or bulk email (spam) which, aside from being a nuisance and a drain on IT resources, might be a means to spread computer viruses and other malicious software. Avoid opening unsolicited messages and report any suspicious email. Delete and block all senders of spam immediately. Do not reply to the message in any way, even if it states that you can request to be removed from its distribution list.

Users should be aware that spammers have the ability to access email addresses that are listed as senders or recipients on email messages, on websites, user discussion groups, and other internet areas. Therefore, you should be cautious about using and disclosing your organization email address. If you use email for information gathering purposes, we strongly recommend that you not use your organization email address, but rather establish a separate email account for that purpose with a free email service, such as yahoo.com, hotmail.com or google.com.

Etiquette. Proper business etiquette should be maintained when communicating via email and text messaging. When writing business email, be as clear and concise as possible. Sarcasm, poor language, inappropriate comments, attempts at humor, and so on, should be avoided. When communicating via email or instant messages, there are no facial expressions and voice tones to assist in determining the meaning or intent behind a certain comment. This leaves too much room for misinterpretation. Email and other written electronic communications should resemble typical professional and respectful business correspondence.

Personal Use of Company-Provided Email. Personal use of organization-provided email is never permitted.

Use of Social Media. The internet provides unique opportunities to participate in discussion groups and activities and share information on particular topics using a wide variety of social media. Social media is technology that enables online users to interact and share information (including video, audio, photographs and text) publicly or privately. APSNA respects the right of any member to use social media. However, to protect the organization's interests and ensure members focus on their duties, members must adhere to the general internet use guidelines and rules in this policy, and the following related specifically to social media use:

- Remember that anything you post or send using social media could reflect on APSNA, in addition to yourself, and might create legal liabilities for APSNA or damage its business or reputation.

- To avoid the risk of the organization incurring legal liability or damage as a result of your use of social media, whether in or outside of your role as a member of APSNA, remember that you are solely responsible for all content that you post or send. APSNA prefers that you avoid identifying yourself as a board member or officer of APSNA, using your APSNA email address or mentioning APSNA unless you receive written instructions or permission from the Secretary to do so. If you do

identify yourself as a board member or officer of APSNA, you may not identify yourself as a representative of APSNA and it is recommended that you include a disclaimer that your views do not represent those of APSNA. For example, consider such language as "the views expressed by me do not represent the views of APSNA". This is necessary to avoid damage to APSNA's reputation and goodwill in the marketplace. Also note, if you endorse APSNA in any way, by law you must disclose your affiliation and role with APSNA.

- You should carefully review APSNA's Social Media Policy for guidelines and restrictions related to all business use of social media. If you are contacted for comment about APSNA for any publication, including any social media outlet, direct the inquiry to the Secretary and do not respond without written approval. Note that APSNA owns all social media accounts used for business purposes on behalf of APSNA, including any and all content associated with each account, such as followers and contacts. APSNA owns all such information and content regardless of the member that opens the account or uses it and will retain all such information regardless of separation of any member from membership or official capacity with APSNA.

- Any conduct that under the law is impermissible if expressed through any other public forum is also impermissible if expressed through social media.

- If you see content in a social media environment that reflects poorly on APSNA or its members, notify the Secretary immediately. Protecting APSNA's goodwill and reputation is part of every member's job.

- Finally, keep in mind the speed at which information can be relayed through social media, and the manner in which it can be misunderstood and distorted by readers and subsequent re-posters. Accordingly, APSNA urges all member not to post information regarding APSNA or their membership that could lead to morale issues in the organization or that might detrimentally affect APSNA's goodwill or reputation.

Inappropriate Use of Company IT Resources and Communications Systems

You are never permitted to use the organization's IT resources and communications systems, including email, text ssaging, internet access, social media, telephones and voicemail, to the extent provided by APSNA, for any inappropriate or unlawful purpose. This includes but is not limited to:

- Misrepresenting yourself as another individual or organization.

- Sending, posting, recording or encouraging receipt of messages or information that may be offensive because of their sexual, racist, or religious content.

- Revealing proprietary or confidential information, including official APSNA information.

- Conducting or soliciting illegal activities.

- Representing your personal opinion as that of APSNA.

- For any other purpose that violates APSNA's policies or practices.

Any person with an apsna.org email, committee chairs, SIG chairs, and members using APSNA resources will adhere to this policy.