



School Administrators Association of New York State

**SAANYS**  
LEGAL DEPARTMENT

8 Airport Park Boulevard | Latham, New York 12110

Phone: (518) 782-0600 | [www.saanys.org](http://www.saanys.org)

## Communication Best Practices

*May 2022 News & Notes*

It is essential to preserve confidentiality when communicating with a SAANYS attorney. This guide is to help association members protect the privacy of their communications while at work. Please note that this guide is not intended to be comprehensive or exhaustive. Additionally, this communication does not and cannot replace personalized legal advice. When in doubt, please call the SAANYS Legal Department at 518-782-0600.

### **Key Concept: Confidentiality v. Attorney-client Privilege**

There are significant differences between confidentiality and attorney-client privilege, but enough overlap exists making it easy to conflate the two concepts. Confidentiality generally relates to an attorney's professional obligation to not reveal confidential client matters to others without authorization. Attorney-client privilege, on the other hand, applies when a client and their attorney communicate confidentially for the purposes of seeking/rendering legal advice. Importantly, attorney-client privilege does not attach to emails sent to SAANYS attorneys when sent via work email because work emails are the employer's property. Rest assured, SAANYS attorneys will never reveal confidential client matters to unauthorized individuals. Clients, however, may inadvertently destroy both confidentiality and attorney-client privilege by communicating with SAANYS attorneys using the employer infrastructure, e.g., the employer's VoIP phone or email.

### **Tip No. 1: Always email SAANYS from a personal email address.**

The SAANYS Legal Department receives many emails from association members' work email addresses. As previously stated, this immediately destroys both confidentiality and attorney-client privilege, because the employer owns the email address, the emails, and the network over which the emails are sent. Therefore, always use a personal email address to protect the privacy of your communications.

### **Tip No. 2: Never use employer Wi-Fi.**

Employers can track information from devices connected to their network (e.g., Wi-Fi). For example, the employer can see the name of the device, the MAC address, and any unencrypted traffic sent over the employer's Wi-Fi, including web searches and communications. For this reason, it is important to avoid using the employer's Wi-Fi. Additionally, because Wi-Fi can be used to track a variety of personal details (including location), employees should disconnect their personal devices from the employer's network. (For further reading, look up "indoor positioning system" or "received signal strength indicator.") This means using a cellular service provider's network (e.g., 5G, 4G/LTE, etc.) or, if at home, home Wi-Fi.

### **Tip No. 3: Never sign into personal accounts on employer devices.**

Never sign into personal accounts on an employer device. In addition to the fact that the employer will see the non-work internet traffic, it opens the employee's life up to scrutiny. Facebook, Google, and other technology platforms track location, log web searches, store photos, and more. Employees who do not wish for their employer to see their entire lives on display should never log into a personal account on an employer device.

#### **Tip No. 4: Be aware of keyloggers.**

Keyloggers are either hardware or software modules and log keystrokes entered on a keyboard. Keyloggers can track length and velocity of each keypress, as well as the identity of the key. Additionally, keyloggers run silently in the background while employees use their computers, so employees will not normally know if a keylogger is tracking their keystrokes. One should assume their keystrokes are always being logged. Importantly, when an employee types something into a computer with a keylogger, every keypress is logged. Therefore, even if an employee types something which they subsequently delete, the keylogger will track all the keypresses—including the deleted material. It is important to think carefully before typing something into a work laptop, because whatever typed may become part of a permanent record.

#### **Tip No. 5: Do not use work email, work phone, etc. for personal use.**

Regular business communications are generally subject to New York Freedom of Information Laws, even if done on a personal device. Therefore, keep work communications separate from your personal devices. If this is impossible, limit the number of work communications to phone calls because the substance of phone calls is generally unrecorded and would therefore not be subject to FOIL. (Things that do not exist cannot be FOIL'd.)

#### **Call SAANYS Legal Department**

When in doubt as to how to preserve confidentiality with a SAANYS attorney, call us (from your personal phone) at 518-782-0600 for assistance.

*“The contents of this communication are intended to convey general information only and not to provide legal advice or opinions. The contents of this communication should not be construed as, and should not be relied upon for, legal advice in any circumstance or fact situation. The information presented in this communication may not reflect the most current legal developments. No action should be taken in reliance on the information contained in this communication and we disclaim all liability in respect to actions taken or not taken based on any or all of the contents of this site to the fullest extent permitted by law. An attorney should be contacted for advice on specific legal issues.”*