Technology Resource Use and Privacy

A. Use of Technology Resources

The Schools Insurance Group provides technology resources to employees, to assist them in performing their job duties. The term "technology resources" refers to all electronic devices, software and means of electronic communication, including but not limited to desk and lap-top computers, computer hardware and software, peripheral equipment such as printers, modems, fax machines, copiers and digital devices such as laptops, cellular phones, tablets, wifi hotspots, and others. Each employee has a responsibility to use the Schools Insurance Group's technology resources in a manner that increases productivity, enhances the School Insurance Group's public image, and is respectful of others. Failure to follow policies regarding technology resource use may lead to discipline, up to and including termination.

Employees may use their personal cellular phones to conduct SIG business, and these devices will be considered dual use equipment. As such, SIG reserves the right to access business-related information on these dual use devices, for objective business purposes and to respond to requests for disclosure under the CA. Public Records Act. These devices may also be subject to discovery during certain instances of litigation to which SIG or a SIG member may be a party. If a dual use device is subject to production and disclosure for discovery, an evidence preservation notice will be provided. Where email or other electronic communications must be preserved during the pendency of a litigation matter, SIG will provide a temporary device for an employee to use while the dual use device is held.

The Schools Insurance Group's technology resources are generally to be used only for the purpose of conducting business for the Schools Insurance Group. Employees' personal use of these resources is limited to authorized break time, when such use (a) does not interfere with the employee's duties; (b) is not done for pecuniary gain; (c) does not conflict with Schools Insurance Group business; and (d) does not otherwise violate any Schools Insurance Group policy. The Schools Insurance Group assumes no liability and accepts no responsibility for any loss, damage, destruction, alteration, disclosure, non-delivery or misuse of any personal data or communications transmitted over or stored in the Schools Insurance Group's technology resources. Use of Schools Insurance Group equipment during a remote work arrangement is addressed in the SIG Remote Work Policy & Procedures.

The separate SIG Remote Work Policy & Procedures for remote workers fully applies to the terms and conditions of this policy, as a component of this Employee Handbook. Each remote worker will be responsible for compliance with all policies contained in this Handbook, in accordance with the separate remote work arrangement between Schools Insurance Group and each individual employee subject to the remote work arrangement.

B. School Insurance Group Access to and Monitoring of Content

All messages sent and received, including personal messages, and all data and information stored on the Schools Insurance Group's technology resources are property of the Schools Insurance Group, regardless of content. As such, the Schools Insurance Group reserves the right to access all of its technology resources, including its computers, voicemail and e-mail systems (email both on SIG owned equipment and dual use cellular phones), at any time and in its sole discretion. The Schools Insurance Group may also monitor its technology resources at any time, in order to determine compliance with its policies, for purposes of legal proceedings, to investigate misconduct, to locate

information, to comply with the CA. Public Records Act (CPRA), or for any other business purpose. Employees should have no expectation of privacy with respect to the information transmitted, received or stored on SIG property or related to SIG business.

C. Passwords and Privacy

Any passwords assigned to or selected by employees in connection with their use of the Schools Insurance Group's technology resources are intended to protect the information on behalf of the Schools Insurance Group, and not the individual employee who has been assigned the password. The Schools Insurance Group will keep copies of all passwords. Employees must not expect that possession of a password entitles them to any privacy with respect to the Schools Insurance Group's access to and right to review material entered or received under that password. Employees are expected to maintain passwords as confidential. Employees are not permitted to share their passwords with unauthorized co-workers or other parties, nor may they access information protected by password without the express authorization of the password-holder and/or their supervisor.

D. Network Security

Computers are critical to the business operations of Schools Insurance Group. Therefore, practice the following precautions when communicating across all devices that may be linked to, or interface with, SIG's network:

Passwords: Safeguard the security of the SIG network against attack from the outside. Under no circumstances should you give your password to another, particularly in response to a request, by phone or email from anyone pretending to have a need for it. (It's remarkable how many systems have been breached by hackers operating under the guise of technicians, system administrators, telephone company workers, etc.)
Alternations to Electronic Network: Neither the hardware nor software configuration may be changed without specific authorizations. Examples of changes requiring authorization include: installing new software or hardware, formatting a hard drive, adding new drivers. To request a change, please make the request to the Executive Director or information technology designee.
Internet Service Providers. All business communications that involve Internet traffic must pass through the SIG network where access controls and related security mechanisms will be applied. All individuals with authorized access to the network are prohibited from bypassing the SIG network, security mechanism, or content filtering policies.
Use of Wireless Devices. PDAs, tablets, smartphones, cellular phones, and other wireless devices that can contain sensitive information must be secured in the same manner as desktop and laptop computers. Devices owned by SIG will be issued and returned according to SIG procedures. Take reasonable and appropriate steps to secure sensitive information while onsite at the SIG office or when working from remote locations.

E. Social Media Code of Conduct

SIG employees may communicate within social media platforms online, for both personal and business purposes. This policy applies to social media communications that take place at the SIG office or from remote work locations. Social media includes all means of communicating or posting information or content of any sort on the Internet, including to your own or someone else's web log or blog, journal or diary, personal web site, social networking or affinity web site, web bulletin board

or a chat room, whether or not associated or affiliated with SIG, as well as any other form of electronic communication**.**

To ensure that SIG employees understand the expectations regarding external social media use, the following conduct guidelines have been developed and adopted. Employees are expected to follow these guidelines using their best personal and professional judgment.

1. Always be fair and courteous to co-workers, member districts, business partners, vendors, suppliers, Board members or people who work on behalf of Schools Insurance Group. If you decide to post complaints or criticism, avoid using statements, photographs, video or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating.

2. Use appropriate and professional judgement in the language used when posting on social media. Do not use language that is, or may be perceived by a reasonable person in the community as intolerant, biased, discriminatory, harassing, bullying, or abusive.

3. Employees are expected to protect the privacy of SIG and its member districts and employees and are prohibited from disclosing personal employee and non-employee information and any other proprietary and nonpublic information to which employees have access. Such information includes but is not limited to customer information, trade secrets, financial information and strategic business plans.

4. SIG Employees are responsible for the content they publish on any form of user-generated media. Be mindful that what you publish will be public for a long time—protect your privacy, and don't say anything online for which you're not willing to be fully accountable.

5. If you publish content to any website outside of Schools Insurance Group that is related to your work for SIG or on subjects associated with SIG or its member districts, use a disclaimer such as this: "The postings on this site are my own and don't necessarily represent the positions, strategies, or opinions of Schools Insurance Group or its members."

6. Refrain from using social media while on work time or on equipment we provide, unless it is work-related. Do not use your SIG business email addresses to register on social networks, blogs or other online tools utilized for personal use.

7. Never publish or disclose confidential or other proprietary information. Never publish or report on business conversations that are meant to be private or internal to SIG.

8. Report any violations or possible or perceived violations to the Executive Director or a Board member. Violations include discussions of proprietary information and any unlawful activity related to blogging or social networking.

9. Schools Insurance Group prohibits taking negative action against any employee for reporting a possible deviation from this policy or for cooperating in an investigation. Any employee who retaliates against another individual for reporting a possible deviation from this policy or for cooperating in an investigation will be subject to disciplinary action, up to and including termination.

10. This policy is not intended to and does not limit or prevent employees from communicating with one another concerning the terms and conditions of their employment or to limit their rights as employees under federal or state laws, including constitutional protections for public employees.

This is where the Telecommuting Policy & Procedure/ remote work arrangement policy should go – and then pick up with the rest of the EE Handbook.