SINGLETON SCHREIBER

INJURY ATTORNEYS

TECHNOLOGY ACCEPTABLE USE PLAN

The enclosed Technology Acceptable Use Plan provides clear guidelines for the responsible and secure use of Singleton Schreiber LLP-provided technology and digital resources. This plan ensures compliance with legal, ethical, and organizational standards while protecting sensitive data and maintaining a productive work environment.

TABLE OF CONTENTS

I. Executive Summary 2
Purpose 2
Scope 2
General Use 2
Definitions 2
1. Sensitive Data 2
2. Approved Artificial Intelligence ("AI") Tools 3
3. Work Product 3
II. Access Control 4
Passwords 4
Remote Access 4
Vendors and Third-Party Access 4
Guest Access 4
Departed Personnel Access 4
III. Computer Equipment and Hardware 5
Lost or Damaged Equipment 5
Personal Mobile and Handheld Devices 5
IV. Software and Licensing 6
V. Electronic Communication 7
Email 7
Delegate Access 7
Suspicious Communications 7
Collaboration Platforms 8
Non-Firm Messaging Tools 8
Voicemail 8
VI. Data Storage 9
VII. Artificial Intelligence ("AI") 10
Acceptable Use 10
Prohibited Use 10
Personnel Responsibilities 11
VIII. Security And Proprietary Information 12
IX. Unacceptable Use Of Technology 13
X. Policy Compliance 15
Compliance Measurement 15
Exceptions 15
Non-Compliance 15

I. EXECUTIVE SUMMARY

PURPOSE

This Acceptable Use Policy ("AUP" or the "Policy") outlines the acceptable use of technology resources provided by Singleton Schreiber LLP ("Singleton Schreiber" or the "Firm"). This AUP applies to all members of Singleton Schreiber, including partners, employees, contractors, consultants, temporary employees, and any other individuals granted access to the Firm's information technology infrastructure.

The purpose of this policy is to outline the acceptable use of computer equipment at Singleton Schreiber. Inappropriate use, either knowingly or unknowingly, exposes Singleton Schreiber to risks including malware attacks, compromise of network systems, data loss, reputational harm, and legal issues.

SCOPE

All on-premises and hosted cloud technologies, including but not limited to computer equipment, software, network accounts, email, voicemail, web browsing, storage media, data, and electronic work product are property of Singleton Schreiber and are for use in carrying out Firm business. This includes the production of client and administrative materials and communications, both internal and external to Singleton Schreiber.

GENERAL USE

Singleton Schreiber's communication and computer systems are intended primarily for business purposes; however, limited personal usage is permitted if it does not hinder performance of job duties or violate any other firm policy. Individuals have no legitimate expectation of privacy regarding their use of Singleton Schreiber systems.

Firm personnel have a responsibility to promptly report the theft, loss or unauthorized disclosure of Singleton Schreiber's proprietary information, or computer equipment. Individuals may access, use, or share Firm proprietary information only to the extent it is authorized and necessary to fulfill assigned job duties and client requirements.

Firm policies prohibiting harassment, in their entirety, apply to the use of all communication and computer systems restricting any use 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.

For security and network maintenance purposes, authorized Singleton Schreiber individuals or contracted support providers, may monitor or audit equipment, systems, and network traffic at any time to ensure compliance with this policy, or at the direction of Firm leadership.

DEFINITIONS

The following definitions shall apply to this Plan:

1. Sensitive Data

Client and firm personnel information classified as confidential, proprietary, or protected by law, including but not limited to personal identifiable information (PII), financial records, and intellectual property.

2. Approved Artificial Intelligence ("AI") Tools

Only Generative AI Tools approved by Singleton Schreiber may be used for client-related work. This ensures that the tools meet Singleton Schreiber's security and compliance standards. Approved AI tools are those designed specifically for use in the practice of law and trained on data sets that are maintained by, and proprietary to, those legal services vendors. These tools differ from publicly available AI tools, such as ChatGPT, Bard, Microsoft Co-Pilot, and other similar products which are trained on data gathered from publicly available data from the Internet, as well as user information and inputs. The IT Department maintains a list of approved AI tools which is updated periodically.

3. Work Product

A writing that reflects an attorney's impressions, conclusions, opinions or legal research or theories (Cal. Civ. Pro. §2018.030). In the context of this policy, work product means any writings generated by firm personnel in connection with advising and counseling clients, preparing for or conducting litigation activities representing a client in transactional work, or providing any other form of legal service to a client.

II. Access Control

Access to systems, data and network resources is authorized by the appropriate Firm personnel. Should access to additional systems and data be required, approval must be obtained from the relevant manager or system owner in advance.

Passwords

Strong passwords shall be used to access Firm systems, in accordance with password policy of a minimum of 10 characters in length that is free of consecutive identical, all-numeric or all-alphabetic characters, and should be protected and only known to Firm personnel when necessary. Each person is responsible for the proper use and protection of their accounts and passwords. Passwords are used for various purposes at Firm, including but not limited to user level accounts, web accounts, email accounts, endpoint protection, voicemail. Passwords will never be transmitted with identifiable data that could link it back to the service for which it is intended.

Remote Access

Remote access to Singleton Schreiber's network is permitted for authorized individuals. Secure connections must be used, and Firm personnel must comply with all security measures in place to protect the confidentiality and integrity of data. Remote access to all Firm systems will require two-factor authentication. Only authorized devices, which meet organization-defined security standards, are allowed to connect remotely.

Vendors and Third-Party Access

All vendors, contractors, consultants, and other third parties conducting business for Singleton Schreiber and requires access to Firm systems and information will agree to certain terms and conditions prior to onboarding. Singleton Schreiber will ensure that these third parties and their policies, procedures and practices conform to those of the Firm.

Guest Access

Guests of Singleton Schreiber will be granted limited and direct wi-fi access to the Internet but are prohibited from access to the Firm’s core systems or production network.

Departed Personnel Access

Access to Firm systems, applications, data repositories, and other network resources will be disabled at either close of business on the individual’s departure date, or as specified by Firm leadership.

III. Computer Equipment and Hardware

All Singleton Schreiber personnel or contracted support providers are issued a computer (laptop) and applicable peripherals, potentially including monitors, webcam, docking station, upon joining Singleton Schreiber. Equipment provided by Singleton Schreiber for office/home use such as firm laptops, or other devices, must be kept in a secure location and use for any other purpose other than Firm business is restricted. Personnel have no expectation of ownership of such equipment, linkages, property, or other items installed or provided by Singleton Schreiber. Laptops are configured to comply with Firm standards for security, uniformity, and operation.

No computers, peripherals, portables, or voice equipment may be reassigned, moved, disposed of, or changed without the express knowledge and approval of IT or firm leadership.

Lost or Damaged Equipment

Firm personnel or contracted support providers take full responsibility for the safekeeping of the equipment. In the event of lost or stolen equipment, personnel must report the incident immediately to the IT department and appropriate authorities, if necessary. Individuals will be responsible for the replacement or recovery costs associated with lost or stolen equipment, excepting fair wear and tear or at fair market value, unless the incident is promptly reported, and the circumstances are beyond the person's control.

Personal Mobile and Handheld Devices

Personal mobile devices must be protected with a password, PIN, biometric authentication features, or other secure authentication method. User-owned mobile devices must be kept up to date with the latest security patches and updates. In the event of loss or theft of the mobile devices, individuals must promptly report incidents to the IT Department so that IT can remotely wipe data from the lost or stolen device to prevent potential unauthorized access.

Firm-sensitive information and data must not be stored on personal cloud services without explicit approval from Firm leadership.

Employees whose job responsibilities include regular or occasional driving are expected to follow all state laws regarding the use of mobile phones while operating a vehicle. Singleton Schreiber expects all employees, regardless of location, to comply with all applicable laws and not text or email while operating a motor vehicle. Under no circumstances are employees allowed to place themselves at risk to fulfill business needs. Employees who are charged with traffic violations resulting from speeding or the use of their cellular phone while driving will be solely responsible for all liabilities that result from such actions.

IV. SOFTWARE AND LICENSING

Singleton Schreiber recognizes the importance of using software legally and ethically. Firm personnel are authorized to use only licensed software and applications which Singleton Schreiber holds valid and appropriately acquired licenses. Downloading of games from the Internet is prohibited and downloading of any executable files or programs which change the configuration of your system by anyone other than IT staff is prohibited. It is mandatory for personnel to comply with copyright and trademark laws when downloading material from the Internet.

Singleton Schreiber accepts no responsibility for software licensing violations that an individual may incur relative to using software that has not been authorized by the IT staff. Any damage that occurs because of downloading software or files should be reported immediately to IT.

Because software transmitted by email frequently contains malicious code or conflicts, some messages with software attachments will be blocked by Singleton Schreiber's anti-spam service. In the event such an attachment that escapes detection is received, please do not open, install, or use any software received via email, including screen savers, games, cartoons, animated attachments, or program files of any type.

Personal software will not be installed on Firm-owned devices.

V. ELECTRONIC COMMUNICATION

Electronic communications include email, instant messaging, chat messages, collaboration platforms, voicemail, video conferencing, and any other form of digital communication used within Singleton Schreiber. Electronic communications are to be used for professional and work-related purposes. Firm personnel should exercise discretion and professionalism in all electronic communications. Use of the Internet, email and other computer resources must always be able to withstand public scrutiny and not cause legal liability or embarrassment to Singleton Schreiber.

Limited personal use of electronic communications is permitted, provided it does not interfere with work duties and adheres to Singleton Schreiber's policies. There should be no expectation of privacy when using Firm-provided electronic communication resources.

EMAIL

Firm personnel are responsible for safeguarding the security and confidentiality of email communications, including emails and messages containing sensitive or confidential information. Encryption and secure channels should be used for transmitting sensitive information whenever possible.

Firm personnel are encouraged to report any suspicious or unauthorized use of electronic communications promptly to the IT department.

Electronic communications may be subject to archiving and retention policies in accordance with legal and regulatory requirements.

DELEGATE ACCESS

Individuals can grant delegate access to their email accounts when necessary due to absence, workload, or other legitimate reasons. Email delegation should be authorized by the individual, or appropriate Firm leader. Delegates are expected to handle the delegated email account responsibly and only perform tasks explicitly authorized by the delegating person. Delegates should not access or disclose information beyond the scope of their delegated responsibilities.

Individuals delegating their email accounts should exercise caution when granting access to sensitive or confidential information. Delegates are obligated to treat any sensitive information encountered during their delegated responsibilities with the same level of confidentiality as the delegating user.

SUSPICIOUS COMMUNICATIONS

Suspicious email communications may include phishing attempts, unsolicited emails with suspicious links or attachments, and emails requesting sensitive information. Firm personnel should exercise caution and scrutiny when encountering emails that are unexpected or seem unusual. Email may contain malicious attachments or links designed to compromise Singleton Schreiber’s computers, data, systems, or other network resources. Some malicious email messages do not contain harmful code, rather they can include instructions for the recipient while impersonating a Firm leader to perform certain actions, such as purchase goods or materials, and relay details of those goods to the sender.

Indicators of suspicious emails include unexpected sender addresses, misspellings, generic greetings, and urgent requests for sensitive information. Avoid clicking on links or downloading attachments from emails that appear suspicious or unexpected. Hovering over links to view the actual URL before clicking can help users identify potentially malicious links.

Firm personnel are responsible for examining electronic communications to ensure they are legitimate before accessing attachments or links. Any suspicious email activity or phishing emails should be reported

to the IT department. Individuals should never disclose sensitive information, such as login credentials or financial details, in response to suspicious email requests. Requests for sensitive information should be verified with Singleton Schreiber's established procedures before providing any details.

COLLABORATION PLATFORMS

Singleton Schreiber offers collaboration platforms that allow Firm personnel to communicate and share information with colleagues within the Firm (i.e., Microsoft Teams, Zoom). Communication channels include instant messaging and chat features. Collaboration platforms are to be used for professional communication only. Collaboration platforms are designated for professional and work-related collaboration within Singleton Schreiber. Firm personnel are responsible for safeguarding the security and confidentiality of information shared on collaboration platforms.

NON-FIRM MESSAGING TOOLS

Non-Firm messaging tools refer to any communication applications or platforms not explicitly authorized or provided by Singleton Schreiber for official business use. This includes personal messaging apps, social media platforms, and other external communication tools. Firm-provided messaging tools and platforms are designated for professional and work-related communication. Firm personnel should refrain from using non-Firm messaging tools for official business purposes, especially when handling sensitive, confidential, and attorney/privileged client information.

Non-Firm messaging tools may not provide the same level of security and confidentiality as Firm-approved platforms. Individuals should exercise caution and avoid sharing sensitive or confidential information on non-Firm messaging tools.

Singleton Schreiber recognizes that clients may require the use of public, non-Firm instant messaging systems to communicate. Individuals are responsible for the content shared on non-Firm messaging tools and must ensure that it aligns with professional standards and Singleton Schreiber's code of conduct. The Firm does not assume ownership or control over data shared on non-Firm messaging tools.

VOICEMAIL

Firm personnel are responsible for safeguarding the security and confidentiality of information shared through voicemail messages. Sensitive information and proprietary business data should not be left in voicemail messages. If it is necessary to convey sensitive information, alternate secure communication methods should be used.

VI. Data Storage

Data created, processed, or stored within Singleton Schreiber's network infrastructure is the property of the Firm. Only authorized personnel are permitted access to firm networks, files, and other information repositories. No data, files, or any information, electronic or otherwise, may be removed from or copied outside Singleton Schreiber's network without authorization. Individuals are obligated to protect and maintain the confidentiality of sensitive and confidential information.

Singleton Schreiber may access data and monitor systems to ensure compliance with Firm policies and procedures, to answer subpoenas or other court orders or client requests, to improve performance and operations, and to investigate Firm matters. There is no right of personal privacy with respect to any information stored on or transmitted by Firm systems.

Firm personnel should store data in approved and secure locations designated by Singleton Schreiber. Access to sensitive data should be restricted based on job roles, and access credentials must not be shared. Sensitive data, especially during transmission, should be encrypted to safeguard against unauthorized access.

Unauthorized access, data breaches, or incidents involving data loss must be promptly to the IT department or Firm leadership.

VII. Artificial Intelligence ("AI")

Singleton Schreiber personnel must ensure AI is applied to enhance and support legal work without replacing critical human judgment and oversight and be used in ways that comply with all applicable laws, regulations, and professional ethical standards. AI tools should only be used for purposes approved by management directly related to the firm's legal services, administrative tasks, or other business functions.

Sensitive client information must be handled with the highest level of confidentiality and security when processed by AI technologies. Singleton Schreiber personnel must ensure that AI tools are used in compliance with data protection regulations, including GDPR, CCPA, and other relevant data privacy laws. Any AI system or tool must be vetted by IT for security vulnerabilities prior to deployment and use and be regularly updated to mitigate potential risks.

With respect to ethical considerations, AI applications must be used by Firm personnel in ways that promote fairness, transparency, and accountability and avoid biases that could result in unfair treatment or discrimination against any individual or group. Decisions informed by AI must be subject to human review, especially in contexts where legal, ethical, or significant business implications are involved.

Acceptable Use

While it is impossible to list all appropriate uses of approved AI tools, the following is a non-exhaustive list of uses of approved AI tools that are generally considered by Singleton Schreiber to be appropriate:

1. Conducting research, including legal research, obtaining general knowledge on substantive issues, and brainstorming ideas
2. Summarizing cases and other legal research materials
3. Creating outlines, presentation materials, internal Firm communications, and other materials created for internal Firm purposes
4. Creating initial drafts of emails, letters, memoranda, and similar written materials
5. Summarizing key terms and provisions of transaction documents
6. Using AI functionality in approved e-discovery platforms such as Everlaw and other such platforms approved by the IT Department

Prohibited Use

The following is a non-exhaustive list of uses of AI tools that are generally considered by Singleton Schreiber to be prohibited:

1. Using unauthorized AI Tools in the course and scope of Firm business
2. Inputting, uploading, or otherwise disclosing Confidential Information or Sensitive Information into any AI Tool
3. Inputting, uploading, or otherwise disclosing to any AI Tool the name of the client(s) for whom legal work is being conducted, or any information that could identify the client, or the client's confidential or proprietary information
4. Relying upon AI Tools to produce work without fully verifying the accuracy of the entire output through sources other than the approved AI Tool
5. Presenting finished work or content directly from AI outputs, including copying and pasting outputs from AI Tools with the purpose of presenting the material as an individual's work product

6. Infringing the intellectual property rights of content creators by copying and using outputs without appropriate attribution
7. Failing to disclose to the lead attorney when approved AI Tools have been used to create work product that will be sent to a client

PERSONNEL RESPONSIBILITIES

1. Firm personnel must undergo training on the ethical and appropriate use of AI tools.
2. Any misuse or unauthorized use of AI tools must be reported immediately to your supervisor or designated authority.
3. Personnel are responsible for ensuring that AI use aligns with Singleton Schreiber's commitment to professional integrity and client trust.

.

VIII. SECURITY AND PROPRIETARY INFORMATION

Singleton Schreiber personnel or contracted support providers are prohibited from allowing other individuals to share credentials or access their account, including the sending of electronic mail from their account and in turn, may not use another account to send e-mail communications for their own purposes. Administrative level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

Proprietary information stored on electronic and computing devices whether owned or leased by the firm, its personnel, or a third party, remains the sole property of Singleton Schreiber.

Appropriate methods for secure transmission or encryption must be utilized for the electronic communication of personal or confidential information. Personally Identifiable Information (PII) should be omitted from unencrypted communications, (i.e., social security numbers, bank accounts).

Outgoing email messages must include a statement to ensure confidentiality:

All computers must be secured with password-protected encryption software and with the automatic lockout feature set to 15 minutes. Firm personnel must lock the screen or log off when the device is unattended.

IX. Unacceptable Use Of Technology

The following activities are, in general, prohibited:

- Violation of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources.
- Unauthorized installation of any copyrighted software for which Singleton Schreiber or the end user does not have an active license.
- Accessing data, user accounts, on-prem servers or cloud resources for any purpose other than conducting Singleton Schreiber business, even if you have authorized access, is prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws.
- Introduction of malicious applications, scripts or software into the network or server (e.g., viruses, worms, Trojan horses, e-mail attacks, keyloggers, etc.).
- Unauthorized use of Artificial Intelligence to fabricate evidence or create/manipulate legal documents.
- Disclosure of account credentials to others or allowing use of your account credentials by others.
- Using a Singleton Schreiber issued device to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- Leaving a Singleton Schreiber issued device in a non-secured area (public area, visible car area, etc.) resulting in theft or damage to the device.
- Liquid spills, or physical damage caused to a Singleton Schreiber issued device resulting in repairs required to restore or replace the device to acceptable working condition. Unless loss or damage arises because of actions outside the individual's reasonable control, individuals agree to reimburse the firm in full for any damage excepting fair wear and tear, or at fair market value for loss or theft.
- Making fraudulent offers of products, items, or services originating from any Singleton Schreiber account.
- Executing any form of network monitoring, port scanning, or security scanning which will intercept data not intended for the employee's host (device) unless this activity is an approved part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network, or account.
- Providing information about, or lists of, firm personnel to parties outside Singleton Schreiber.
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Reading, intercepting, copying, using, or disclosing email communications directed to others without express authorization from firm leadership or immediate supervisor.

- Creating, disseminating, or accessing content that is discriminatory, harassing, defamatory, or otherwise violates Singleton Schreiber's policies or the transmission of offensive, inappropriate, or unlawful content.
- Engaging in activities such as spamming, phishing, unauthorized mass distribution of information or any other form of malicious activity through electronic communications.

X. Policy Compliance

Compliance Measurement

Information Technology staff will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback provided to the policy owner. Singleton Schreiber may access the voice mail and e-mail systems and obtain the communications within the systems, including past voice mail and e-mail messages, without notice to users of the system, in the ordinary course of business when the firm deems it appropriate to do so.

The reasons for which Singleton Schreiber may obtain such access include but are not limited to maintaining the system; preventing or investigating allegations of system abuse or misuse; assuring compliance with software copyright laws; complying with legal and regulatory requests for information; and ensuring firm operations continue appropriately during an individual's absence. Further, Singleton Schreiber may review Internet usage to ensure that such use with firm property or communications is appropriate.

Exceptions

Any exception to this policy must be approved by firm leadership.

Non-Compliance

Singleton Schreiber personnel or contracted support providers found to have violated this policy, or any section of the policy, may be subject to disciplinary action, up to and including termination of employment.

Effective Date: March 7, 2025
Review Date: March 7, 2026
Revision Date: N/A
Approval: Richard Garrett (Technology Director)
Change Summary: N/A