TECHNOLOGY USAGE POLICY

WE USE TECHNOLOGY APPROPRIATELY.

The use of Company automation systems, including computers, and all forms of Internet/Intranet access, is for Company business purposes only. Personal use is permitted as long as it complies with this usage policy. Emery Sapp and Sons is not liable for the loss of personal information and is not required to assist in its recovery or delivery. Any attempts to recover personal information are made on a "best effort" basis and are at the discretion of IT management.

This policy applies to all uses of the Internet, but does not supersede any state or federal laws, or Company policies regarding confidentiality, information dissemination, or standards of conduct.

Employees are individually liable for any and all damages incurred as a result of violating Company security policy, copyright, and licensing agreements.

All Company policies and procedures apply to employees' conduct on the Internet, especially, but not exclusively, relating to: intellectual property, confidentiality, Company information dissemination, standards of conduct, misuse of Company resources, anti-harassment, and information and data security.

Violation of these policies and/or state and federal laws can lead to disciplinary action, up to and including termination and possible criminal prosecution.

INAPPROPRIATE USE OF THE INTERNET/INTRANET

Use of a Company computer, network, or Internet resource to access, view, transmit, archive, or distribute racist, sexist, threatening, or otherwise objectionable or illegal material is strictly prohibited. "Material" is defined as any visual, textual, or auditory item, file, page, graphic, or other entity. Such material violates the Company's anti-harassment policies and is subject to Company disciplinary action.

Employee-owners are prohibited from using the Company's Internet/Intranet facilities to engage in activities that disrupt users, equipment, or services; intentionally spread viruses and/or malicious programs; provide unauthorized access to IT resources; or install software, applications, or hardware that would harm either the Company's networks or systems or those of any other individual or entity.

Your access may be revoked at any time for inappropriate conduct, including, but not limited to:

- **Misrepresenting oneself or the Company**
- **Engaging in unlawful or malicious activities**
- **Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages**
- **Sending, receiving, or accessing pornographic materials**
- **Causing congestion, disruption, disablement, alteration, or impairment of Company networks or systems**
- **Infringing in any way on the copyrights or trademark rights of others**
- **Defeating or attempting to defeat security restrictions on company systems and applications**

OWNERSHIP AND ACCESS OF ELECTRONIC MAIL AND COMPUTER FILES

The Company retains ownership of all data and files within its computers, networks, and other information systems. It reserves the right to monitor computer and email usage, both in real-time and through account histories and their content. Additionally, the Company has the authority to inspect any files stored on the network or any type of computer storage media, whether local or cloud-based, to ensure compliance with this policy and applicable state and federal laws.

The Company will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual computer and email activities. The Company also reserves the right to monitor electronic mail messages and their content. Employee-owners must be aware that the electronic mail messages sent and received using Company equipment are not private and are subject to viewing, downloading, inspection, release, and archiving by Company officials at all times. No team member may access another employee-owner's computer files or electronic mail messages without prior authorization from either the employee-owner or an appropriate Company representative.

Use of Company resources for illegal activity can lead to disciplinary action, up to and including dismissal and criminal prosecution.

INTERNET/INTRANET SECURITY

The Company has taken the necessary actions to ensure the safety and security of our network. Any employee who attempts to disable, defeat, or circumvent Company security measures is subject to disciplinary action, up to and including immediate termination.

SOCIAL MEDIA POLICY

WE'RE SMART AND RESPECTFUL ONLINE.

Social media is a powerful—and sometimes dangerous—tool. Facebook, Instagram, and others are places where we can help build our communities, exchange ideas, and share diverse views and experiences. They're also places that can get you in trouble, fast. The internet never forgets. One mistake could cost you your reputation.

We want you to be able to talk openly about issues that matter to you. But you've got to be smart. It's important to always conduct yourself respectfully.

Be yourself. Be respectful. Use common sense.

TOP 10 SOCIAL MEDIA TIPS

01 Follow the law. Internet postings must respect copyright, privacy, fair use, financial disclosure, and other applicable laws. Also, if you are discussing a Company client, you must disclose that they are a client. We recommend adding #client or a similar disclosure to posts.

02 Don't disclose confidential or proprietary information. Be careful not to reveal any sensitive information about the Company or its clients. This includes information shared on internal sites. Do not reference or discuss client work that has yet to debut. Adhere to all client non-disclosure agreements.

03 Don't claim to speak on the Company's behalf. Employee-owners should neither claim nor imply that they are speaking on the Company's behalf. If there's any doubt, add a disclaimer, such as, "The views expressed are mine alone and do not necessarily reflect the views of ESS and its family of companies." The Company reserves the right to request that employee-owners avoid certain subjects, withdraw certain posts, and remove inappropriate comments.

04 Don't argue. If employee-owners encounter a situation while using social media that threatens to become antagonistic, please disengage from the dialogue in a polite manner and seek the advice of a supervisor.

05 Don't be a jerk. Don't use racial slurs, personal insults, obscenity, or engage in any conduct that would not be acceptable in the workplace. You should also show proper consideration for the privacy of others and for topics that may be considered objectionable or inflammatory, such as religion and politics.

06 Don't make yourself, or the Company, look bad. The line between personal and work discussions online is becoming less clear, so manage your reputation. You are always an ambassador for our Company.

07 Think about the consequences. Using your public voice to trash or embarrass your employer, your clients, your fellow employee-owners, or even yourself is not okay, and not very smart. Please do not reference current or past clients in a negative light.

08 Review before you post. You are personally responsible for the content you publish on blogs, wikis, or any other form of user-generated media. If you are about to publish something that makes you even the slightest bit uncomfortable, please review. If you are still unsure and it is related to the Company, send to your supervisor, or a member of the HR or marketing teams.

09 Get permission to tag others. Please do not tag the Company's executive leadership or other employee-owners in a social media post without their approval.

10 Share your work. If you have relevant, accurate information to share about the Company, do it. Just be smart about it.