Acceptable Use of Electronic Communications

The following policy is lengthy, and the technical jargon might be a little intimidating, but the main purpose is to make sure all employees are aware of the following points:

1. Computers, cell phones, and other electronic devices ("systems") used for business purposes at APC are monitored and there should be no expectation of privacy.
2. While at work, these systems (whether they're owned by APC or you're using your personal device for work) should only be used for legitimate APC business.
3. You should limit any personal use of APC systems to break times, and avoid activities that use excessive resources, like streaming music.
4. You are responsible for securing the data you access at work and ensuring it is appropriately used. You are never permitted to download, copy, save, send, or otherwise remove data from our systems without company approval.
5. When e-mailing client information, you must use encryption to safeguard it. Client information is always confidential- remember HIPAA! Talk to your supervisor if you need instruction on encrypting your messages.
6. Never use our systems for any activity that is illegal or in violation of this policy or any of our other policies; doing so will result in disciplinary action.

This policy contains guidelines for electronic communications created, sent, received, used, transmitted, or stored using the company's communication systems or equipment and employee provided systems or equipment used either in the workplace, during working time or to accomplish work tasks. "Electronic communications" include, among other things, messages, images, text data or any other information used in e-mail, instant messages, text messages, voice mail, fax machines, computers, personal digital assistants (including Blackberry, iPhone, iPad or similar devices), pagers, telephones, cellular and mobile phones including those with cameras, Intranet, Internet, back-up storage, information on a memory or flash key or card, jump or zip drive or any other type of internal or external removable storage drives. In the remainder of this policy, all of these communication devices are collectively referred to as "systems."

Acceptable Uses of Our Systems: Employees may use our Systems to communicate internally with co-workers or externally with clients and other business acquaintances for business purposes.

Company Control of Systems and Electronic Communications: All electronic communications contained in company systems are company records and/or property. Although an employee may have an individual password to access our systems, the systems and electronic communications belong to the company. The systems and electronic communications are accessible to the company at all times including periodic unannounced inspections. Our systems and electronic communications are subject to use, access, monitoring, review, recording and disclosure without further notice. Employee communications on our system are not confidential or private.

The company's right to use, access, monitor, record and disclose electronic communications without further notice applies equally to employee-provided systems or equipment used in the workplace, during working time, or to accomplish work tasks.

Personal Use of Our Systems: Personal communications in our systems are treated the same as all other electronic communications and will be used, accessed, recorded, monitored, and disclosed by the company at any time without further notice. Since all electronic communications and systems can be accessed without advance notice, employees should not use our systems for communication or information that

employees would not want revealed to third parties. Personal use of our system should be limited to non-working time. Personal use of our system must be conducted in such a manner that it does not affect smooth system operation or use a disproportional amount of the system's functional capacity.

Proprietary Business Information: Proprietary business information means confidential and proprietary information related to the company's trade secrets, business models, business services, sales agreements, pricing information, drawings, designs, client lists, vendor agreements, client records, strategic business or marketing plans, expansion plans, contracts, non-public financial performance information and other information that derives economic value by being protected from public consumption or competitors may only be used on company systems. Proprietary business information may not be downloaded, saved, or sent to a personal laptop, personal storage device, or personal email account under any circumstances without advance written approval from a member of management. Proprietary business information does not restrict employee rights to discuss their wages, hours or other terms of employment.

Client Information and Email Encryption: APC employs an e-mail encryption service to ensure that sensitive data or PHI that is transmitted to outside recipients is secure during the sending process. When emailing PHI to recipients outside of APC, employees are required to encrypt messages by typing [encrypt] in the subject line of their email.

Prohibited Uses of Our Systems: Employees may not use company systems in a manner that is unlawful, wasteful of company resources, or unreasonably compromises employee productivity or the overall integrity or stability of the company's systems. These tools are provided to assist employees with the execution of their job duties and should not be abused. Examples of prohibited uses include, among other things, sexually explicit messages, images, cartoons, or jokes; propositions or love letters; ethnic or racial slurs; or any other message or image that may be in violation of company policies.

In addition, employees may not use our company systems:

- To download, save, send or access any discriminatory, obscene, or malicious or knowingly false material;
- To download, save, send or access any music, audio or video file unless business related;
- To download anything from the internet (including shareware or free software) without the advance written permission of the systems supervisor;
- To download, save, send or access any site or content that the company might deem "adult entertainment;"
- To attempt or to gain unauthorized or unlawful access to computers, equipment, networks, or systems of the company or any other person or entity;
- In connection with any infringement of intellectual property rights, including but not limited to copyrights;
- In connection with the violation or attempted violation of any law; and
- To transmit proprietary business information or client material such as pricing information or trade secrets.

Electronic Forgery: An employee may not misrepresent, disguise, or conceal his or her identity or another's identity in any way while using electronic communications; make changes to electronic communications without clearly indicating such changes; or use another person's account, mail box, password, etc. without prior written approval of the account owner and without identifying the actual author.

Intellectual Property Rights: Employees must always respect intellectual property rights such as copyrights and trademarks.

System Integrity, Security, and Encryption: All systems passwords and encryption keys must be available and known to the company. You may not install password or encryption programs without the written permission of your supervisor. Employees may not use the passwords and encryption keys belonging to others.

Applicable Laws: Numerous state and federal laws apply to electronic communications. The company complies with applicable laws. Employees also must comply with applicable laws and should recognize that an employee could be personally liable and/or subject to fine and imprisonment for violation of applicable laws.

Consequences of Policy Violations: Violations of this policy may result in disciplinary action up to and including immediate termination of an employee's employment as well as possible civil liabilities or criminal prosecution. Where appropriate, the company may advise legal officials or appropriate third parties of policy violations and cooperate with official investigations. We will not, of course, retaliate against anyone who reports possible policy violations or assists with investigations.

If you have questions about the acceptable use of our systems or the content of electronic communications, ask your supervisor for advance clarification.

Employer Monitoring