Section 526

Cell Phones and Personal Communication Devices

BACKGROUND

Most employees carry a personal cell phone, smartphone, tablet, or other personal communication device (PCD). Generally, these devices are equipped with features such as cameras, Internet access, texting, applications, and e-mail access.

Although many employers have policies in place that govern the use of company-owned computers and phones, employers should be sure their policies also reflect their standards for appropriate use of PCDs in the workplace. Policies must be reasonable so they can be implemented readily and enforced consistently. The kinds of restrictions imposed in a PCD policy will vary based on the size of the workforce, the employer's business, security needs, and other factors.

This section also includes sample policies related to employees' use of personal audio players in the workplace. Personal audio players typically are used to play music and other stored audio files.

TIPS AND CONSIDERATIONS

- **Coverage.** What kinds of PCDs are included in the policy? Employers may wish to include examples of devices covered by the policy (e.g., cell phones, smartphones, tablets). Does the policy apply to all employees? Only to those who work in areas with proprietary or confidential information?

- **Business needs.** If employees need PCDs to effectively carry out their jobs, employers should consider issuing company-owned PCDs. Employers generally are

Rev. 11/13 (31500033)

978-1-55645-419-6/83/$.50+$.50

permitted to monitor company-owned equipment to ensure that employees are using the equipment appropriately and for business purposes. If an employer provides notice that such monitoring will occur and that employees should not consider their messages private, it may be easier to take disciplinary action against an employee who violates company policy. It is important to actually monitor messages on occasion so that employees do not develop an expectation of privacy.

- **Safety.** If employees are distracted or cannot hear safety instructions because they are using a personal communication device or music player, the employer may be violating the Occupational Safety and Health Administration's (OSHA) requirement for a safe workplace. Employers may wish to adopt more stringent electronic communications policies for employees in safety-sensitive positions. For some jobs, employers will prohibit the use of communications devices to avoid creating unsafe working conditions. Most employers have policies prohibiting employees from using cell phones and similar devices while driving (**see Section 870—Cell Phone Safety**).

- **Emergencies.** Use of PCDs may be the only way to communicate in an emergency when voice lines may be inundated with calls.

- **Coordination with other policies.** An employer should ensure that its policy governing employees' use of PCDs coordinates with its existing policies on telephone use, privacy, professional conduct, safety, discrimination, harassment, and workplace etiquette.

- **Training.** It is important to train managers and supervisors when implementing a policy on employees' PCDs. As with any policy, enforcement should be consistent to avoid claims of harassment, discrimination, or retaliation.

LEGAL POINTS

- **Privacy.** Several states have enacted statutory or constitutional provisions guaranteeing their citizens the right to privacy from certain intrusions. In the absence of a state constitutional provision or existing law, private employees enjoy relatively little freedom from workplace intrusion. However, common law and case law provide employees with some privacy protections, including the following:

  —**Intrusion into an individual's private solitude or seclusion.** An employee may allege this form of privacy invasion when an employer unreasonably searches (e.g., a locker or desk drawer) or conducts surveillance (e.g., dressing rooms) in areas in which an employee has a legitimate expectation of privacy. An employee may have a legitimate expectation of privacy in his or her personally owned communications device. In contrast, a device issued by an employer generally will have a lowered expectation of privacy if it belongs to the employer and is intended for business use only.

Rev. 11/13 (31500033)

978-1-55645-419-6/83/$.50+$.50

—**Use of an individual's name or likeness.** When an employer uses an employee's photograph, likeness, or attributes specific statements to an employee without his or her permission, an individual may have a valid misappropriation claim (e.g., the employer publishes an employee's photograph or likeness on company brochures without first obtaining the employee's consent). The overriding principle governing such claims is that an individual has an exclusive right to his or her identity. To prevent such claims, employers should obtain a release from the employee before using his or her name or likeness.

—**The Electronic Communications Privacy Act of 1986 (ECPA)** prohibits the unlawful and intentional interception of any wire, oral, or electronic communication (18 U.S.C. 2510 *et seq.*; 18 U.S.C. 2701 *et seq.*). Title II of the ECPA, the Stored Communications Act (SCA), also prohibits access to such information while in electronic storage.

• **Harassment.** Employers have an obligation to protect their employees from harassment of all types. PCDs carry the risk of the instant transmission of harassing or embarrassing photographs to other phones, tablets, or to the Internet. Harassment policies should also prohibit the playing of music on personal devices that contain terms derogatory to a specific gender, race, or nationality. This can be construed by coworkers as sexual or racial harassment.

• **Security.** Employers must be concerned with protecting the security of confidential and proprietary information that may be intentionally or inadvertently photographed by employees. In addition to a policy regulating use of PCDs in the workplace, employers should take steps to ensure that confidential information is not located where it can be easily photographed or recorded.

• **Copyrights/piracy.** Employees may use the company Internet connection and computers to download or upload music or videos to or from their personal communication or music devices and thus violate copyright laws. The legal risks of employees downloading music or videos while at work include possible injunctions, damages, costs, and even criminal sanctions against the companies and their directors where company systems are used for copyright theft. It is possible that employers could be liable for such violations. For more information, **see Section 1185—Copyrights.**

• **Instant messaging.** Instant messages are well suited for transmitting short amounts of information or written communication that needs to be received immediately, such as addresses, telephone numbers, purchase order numbers, delivery times, etc. The instant message can be "cut and pasted" into electronic databases.

• **"Bring Your Own Device" (BYOD).** BYOD describes the scenario in which employees use their own devices to do their jobs and use the organization's data or information systems in the process. As technology advances, more and more employees are buying smartphones, tablets, etc., and they want to use them for work purposes. Employers need to consider all the issues that go along with BYOD before allowing their employees to bring and use their own devices for work purposes.

Rev. 11/13 (31500033)

978-1-55645-419-6/83/$.50+$.50

SAMPLE POLICIES

Subject: **Personal Communication Devices**

Example of: Standard Policy

[Organization Name] recognizes that cell phones, smartphones, tablets, and other personal communication devices have become valuable tools in managing our professional and personal lives. However, use of these devices in the workplace can raise a number of issues involving safety, security, and privacy. Therefore, [Organization Name] has adopted the following rules regarding the use of personal communication devices in the workplace during working hours.

- Except in cases of emergency, employees should conduct personal business during lunch breaks and other rest periods. This includes the use of personal communication devices (including cell phones) for personal business (including personal phone conversations and text messages, personal e-mails, and use of the Internet for personal reasons). Employees should be considerate of their coworkers and keep ring tones and alerts on vibrate or silent while at work. Phone calls made during an employee's lunch break or rest period should be made away from the employee's desk or workstation so as not to disturb coworkers. Minimal or incidental use is permitted (e.g., child confirming safe arrival at home after school).

- When attending a meeting with customers, clients, or coworkers, employees should turn off or silence their cell phones and personal communication devices. Except in extraordinary circumstances (e.g., family emergency), employees may not respond to personal calls during a meeting.

- Employees are prohibited from using a device's camera to take photographs in the workplace. Phones and other devices with cameras or recording capabilities are strictly prohibited in all work areas that contain proprietary information or confidential documents [specific information may be included about work areas where cameras are prohibited]. Camera phones and other devices with photographic or recording capabilities may not be brought into restrooms, locker rooms, or other private areas in the workplace.

- Making discriminatory or harassing comments to coworkers via any electronic means of communication is prohibited. This includes offensive messages, photos, or images that are sexual in nature or that are offensive to a person based on his or her race, color, religion, national origin, gender, sexual orientation, disability, or any other characteristic protected by federal, state, or local law. [Organization Name]'s policies on professional conduct, discrimination, and harassment apply to all electronic communications to its employees, customers, clients, and vendors.

Violation of this policy may result in discipline, up to and including termination of employment.

Rev. 11/13 (31500033)

978-1-55645-419-6/83/$.50+$.50

Subject: **Bring Your Own Device (BYOD)**

Example of: Standard Policy

[An organization's BYOD policy (if it has one) will be unique to its organization and its particular needs and circumstances. The following is an overview of some important points and provisions you may want to include when developing your own policy.]

[Organization Name] allows employees to use their personally owned devices for work purposes in certain circumstances. Such devices include, but are not limited to, laptops and other computers, cell phones, smartphones, and tablets.

Access to and continued use of network services is granted on the condition that each employee reads, signs, respects, and follows the organization's policies concerning the use of these devices and services.

Eligibility. [Organization Name] must approve and authorize the use of personal devices for work purposes in writing, and only certain employees may be entitled to use their personal devices. Eligibility will be determined by _____. The use of personal devices may also be limited by device support limitations.

Privacy. Employees have no expectation of privacy in personal devices used for work purposes and should not presume any more privacy than is granted by law. [Organization Name] has the right to monitor and preserve corporate communications and data, including data residing on an employee's personal device used for work purposes. Employees may not knowingly disable network software or systems identified as a monitoring tool.

[Organization Name] reserves the right to review, preserve, or release data on personal devices to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings or investigations.

[Organization Name] reserves the right to require employees to produce their personal devices for inspection upon a legitimate request.

Storing corporate information. Employees are not allowed to download, transfer, or store any sensitive corporate information on their personal devices. Employees agree to delete any sensitive corporate information that may be inadvertently downloaded and stored on such devices through the process of viewing e-mail attachments.

Sharing the device. Employees agree that their personal devices used for work purposes will not be shared with other individuals or family members, because of the business use of such devices.

Reimbursement. In some cases, employees may be eligible for reimbursement for expenses related to their personal devices.

[Insert your organization's policy regarding reimbursement. For example, reimbursement may involve stipends that can be used toward plans, or employees could be reimbursed for device purchase and/or replacement.]

Rev. 11/13 (31500033)

978-1-55645-419-6/83/$.50+$.50

Overtime. All overtime must be preapproved. Additionally, nonexempt employees may not use their personal devices for work purposes outside their normal work schedule without authorization.

Unpaid leave. Employees may not use their personal devices for work purposes during intervals of unpaid leave without authorization.

Use. Employees must use the same discretion in using their personal devices for work purposes as is expected for using organization-owned devices and software. Organization policies, including, for example, those related to safety, discrimination, harassment, ethics, retaliation, trade secrets, and other confidential information, apply to the use of personal devices used for work purposes.

Employees must abide by all applicable state and federal laws and regulations regarding the use of electronic devices.

Security. [Organization Name] has certain security requirements regarding personal devices used for work purposes. Authorized employees must have certain security measures installed on their personal devices they use for work purposes. These security measures are as follows:

[Insert your organization's security requirements. For example, you may require employees to have antivirus and/or mobile device management software installed on their devices. Your organization may also want to bar employees from modifying their device hardware or operating software beyond routine updates.]

Passwords and encryption. Additionally, [Organization Name] has the following password and/or encryption requirements:

[Insert your organization's password and/or encryption requirements. For example, you should address whether encryption is required and/or what happens when there is a failed login.]

"Remote wiping." Employees are to protect their personal devices used for work purposes and should make every effort to prevent them from being lost, stolen, damaged, or subject to unauthorized access. Employees must notify _____ immediately if their devices are lost, stolen, damaged, or subject to unauthorized access.

In order to make sure sensitive organization data are safe, employees must have software that facilitates a "remote wipe" installed on their device. Before an employee uses a personal device for work purposes, _____ will install such software. Such "remote-wipe" software allows organization-related data to be erased remotely if a device is lost or stolen.

Employees who are allowed by the organization to use their personal devices for work purposes agree that the organization may remotely wipe such data if their device is lost, stolen, damaged, or subject to unauthorized access. Employees also agree that the organization may remotely wipe such personal devices when they cease to be employed by the organization.

Such remote wiping may affect other data or applications. [Organization Name] is not responsible for any personal data or applications that are lost or impaired due to remote wiping.

Rev. 11/13 (31500033)

978-1-55645-419-6/83/$.50+$.50

Software agreement. Employees may be required to sign an additional written agreement that discloses all risks associated with organization-required software installed on their devices.

Software upkeep and updates. Employees agree to maintain the original device operating systems and keep the devices current with security patches and updates. Employees agree to install periodic updates to organization-required software. Such required updates will be determined by _____.

Employees will not "jail break" their personal devices used for work purposes by installing software that allows them to bypass standard built-in security features and controls.

Device support. The organization provides the following support for personal devices used for work purposes:

[Insert the details regarding the support your organization will provide and how to request support.]

Cessation of employment. Employees who resign or whose employment is terminated will be asked to produce personal devices they used for work purposes for inspection. The organization will remove all organization data on such devices at the end of employment. Such removal may include remote wiping of personal devices.

Policy violations. Violation of this policy may result in discipline, up to and including termination of employment.

Authorization. Employees who have not been authorized in writing and who have not provided written consent to these policies and requirements regarding use of personal devices for work purposes will not be allowed to use such personal devices for work purposes.

Subject: **Instant Messaging**

Example of: Standard Policy

All communications, including instant messages that are transmitted, received, or stored on [Organization Name] equipment (e.g., computer, modem, software, network, telephone lines, Internet service provider) are the sole property of the company. Accordingly, [Organization Name] may access and monitor employee instant messages.

The use of passwords does not imply any privacy. The systems administrator can override personal passwords. Employees must not disclose their codes or passwords to others. All passwords and all software used to encrypt instant messages are considered company property. Employees may not use personal encryption software for instant messages sent using [Organization Name] equipment.

All instant messages are captured by system software and are subject to review by management. [Organization Name] reserves the right to disclose the content of instant messages to third parties without notice to employees.

Rev. 11/13 (31500033)

978-1-55645-419-6/83/$.50+$.50

Use of [Organization Name] equipment to send instant messages grants consent to use of software to capture content of instant messages and to review and disclose instant messages.

Use of Instant Messaging

Employees' use of instant messaging should be limited to work-related matters, except for incidental personal use. Incidental personal use of instant messaging by employees is permitted as long as the use does not interfere with the employee's work, the company's operations, or the use of communication equipment, and does not violate any policies.

When sending an occasional personal instant message, an employee must indicate that it is personal and not authorized by the company. Employees should not use the instant message system to "visit" with colleagues about non-work-related subjects.

Generally, external instant messages are limited to employees who telecommute, employees who travel, as well as key vendors and customers, as part of a just-in-time delivery system. Outsiders who use the instant messaging system are to be provided a copy of this policy.

When using instant messaging, employees are to follow company security procedures, including use of approved antivirus software.

Employees should not use instant messaging to transmit confidential, proprietary, or trade secret information, or personnel information. Instant messages generally are not an acceptable way to ask permission to leave early or to report that you will arrive late. When voice lines are not available in an emergency, instant messages may be sent instead.

Instant messages are not to be used as a substitute for oral communication with nearby coworkers or telephone calls to key vendors or customers. Generally, verbal communications are preferred when practical.

Instant messages must not be used to create contracts.

Improper Use

Improper use of instant messages may result in discipline, up to and including discharge. Improper use includes, but is not limited to:

- Foul, inappropriate, or offensive messages, such as racial, sexual, or religious slurs;
- Harassing or illegal messages;
- Demeaning, insulting, defaming, intimidating, or sexually suggestive messages;
- Unauthorized codes, passwords, or other means to gain access to others' computers to send messages;
- Instant messages using another employee's identity;
- Chain messages and sports pools;

978-1-55645-419-6/83/$.50+$.50

- Solicitation for outside business ventures, personal parties, social meetings, charities, membership in organizations, political causes, religious causes, or other matters not connected to the company's business; *and*
- Any use that violates company policies.

Subject: **Small Music Players**

Example of: Standard Policy

Employees may listen to music quietly, but the volume must be kept low (including in headsets) so that it does not block out voices or disturb coworkers.

Employees must not walk around the facility, attend internal meetings, or meet with customers, vendors, or servicepeople while listening to personal music devices or wearing headphones, earbuds, etc.

When discussing work-related matters with a manager, supervisor, or any other employee or customer of the company, no matter how briefly, employees must remove their headphones, earbuds, etc.

Use of the company's computers or other facilities to record, upload, or download music is strictly prohibited.

The company's Internet use, copyright, harassment, and other applicable policies apply to music and music players.

The company is not responsible for damage to or loss of any personal music player.

Employees who violate this company policy are subject to discipline, including termination.

Subject: **Personal Music Players**

Example of: Progressive Policy

Employees are expected to use personal music players in a responsible manner that does not interfere with the quality or quantity of their work.

Employees may not listen to music while working, especially with earbuds or headphones, if it poses a safety hazard. Consult your manager with any questions.

If listening to a personal music player causes any problems, the employee will be prohibited from using it on the job.

Rev. 11/13 (31500033)

978-1-55645-419-6/83/$.50+$.50