



Computer And Email Policies

1. *The problem*

Modern electronic technology has vastly increased efficiency in the employment setting. At the same time, it has vastly increased the ease with which employees can engage in personal business, misappropriate company information, engage in inappropriate workplace conduct, and create liability on behalf of the employer. Examples include:

- a. Sexual harassment – e.g. viewing porn sites in the workplace, sending harassing emails.
- b. Using email to conduct inappropriate communication/business
 - o Stealing secrets, conducting competing/side business
 - o Defamation
 - o Tarnish company image
- c. Personal issues on company time
- d. Violation of copyright laws

2. *Overview of Right to Privacy*

Because employees tend to use company technology for inappropriate personal purposes, the control and prevention of such abuses requires an awareness of employees' privacy rights. The California Constitution provides citizens with an inalienable right to privacy. Common law, contract, and statutory rights may also create privacy rights.

(a) Article I, section I, of the California Constitution

"All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, **and privacy.**"

(b) Common Law Privacy. At common law (that is, law created by the courts), invasion of privacy is a tort claim. The four types of invasion of privacy include: unauthorized appropriation of an individual's name or likeness; unreasonable intrusion into an individual's private affairs; public disclosure of private facts; placing an individual in a false light in the public eye.

(c) Contractual Right to Privacy. Handbooks may provide representations regarding privacy that may form the basis of a contractual right. Further, collective bargaining agreements (CBAs) may contain privacy rights.

(d) Statutory Rights

- Federal Safe Streets Act – bans interception of wire, oral, or electronic communication, including email. It includes a ban on recording conversations or communications. Consent to monitoring by at least one party will avoid liability. Liability is also avoided for “extension telephones” used in the ordinary course of business (not used for personal use).

- California Privacy Act. Prohibits wiretapping, eavesdropping or recording a confidential conversation without consent of all parties, interception of cell phone conversations, use of an extension telephone, and the use of a video recorder.
 - Federal Electronic Communications Privacy Act (Wiretap Act and Stored Communications Act) prohibits unauthorized access to or retrieval of a wire or electronic communication, including a stored communication.
 - California Penal Code §653n prohibits use of two-way mirrors permitting surreptitious viewing of any restroom, toilet, bathroom, washroom, shower, locker room, fitting room or hotel room.
- (e) Privacy in the workplace. Employees have workplace privacy rights. An invasion of those privacy rights may lead to legal liability.

(i) General Invasion of Privacy. A person's constitutionally prohibited invasion of privacy, is established by showing: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy." Hill v. National Collegiate Athletic Assn. (1994) 7 Cal.4th 1, 39-40.

(ii) Workplace privacy.

- Key workplace issue is whether an employee has a “reasonable expectation of privacy.”
- Another key issue is balancing an employee's expectations of privacy against the employer's needs to regulate the conduct of its employees at work.
- Reasonable expectation of privacy may exist in employee areas given over to his or her exclusive use, unless the employer gives the employee notice that searches may occur from time to time for work-related purposes.

3. *The solution:* disclosure of policy and employee waiver of certain privacy rights.

(a) Example: An employee may waive his or her privacy rights and may therefore not have a reasonable expectation of privacy, as concerns, for example, the contents of a computer furnished by an employer, whether that computer is located at the workplace or at the employee's home. TBG Ins. Services Corp. v. Superior Court, 96 Cal. App. 4th 443. In TBG, an executive who was fired by an insurance company brought a wrongful termination action against the company, alleging that he was fired in order to prevent his stock holdings in the company from vesting. The reason defendant gave for plaintiff's termination was that he had violated defendant's electronic policies by accessing pornographic Web

sites while he was at work. Plaintiff had been provided with a computer for use at work and another for working at home, and in signing defendant's policy statement, he had agreed to use the computers only for business purposes and not for improper, obscene, or other inappropriate purposes. The employee signed his employer's "electronic and telephone equipment policy statement" and agreed in writing that his computers could be monitored by his employer, the employee fully and voluntarily relinquished his privacy rights in the information he stored on his home computer. Defendant moved to compel plaintiff to produce the home computer. Plaintiff opposed the motion, claiming that the computer contained personal information, and that production of the computer would invade his constitutional right of privacy. The court ruled that because of the disclosure and waiver, the employee reasonable expectation of privacy.

(b) Key policy/waiver terms:

(i) Advance notice to employee about employer's policy. The employer may access its technology, including email, computer files, voicemail, etc at any time. It may monitor the use of its technology at any time for any business purpose without notice. Employees have no right to privacy with respect to any data or messages created, stored, or transmitted on company equipment, including personal information or communications.

- Employee handbook disclosure
- Signed acknowledgment

- Terms:
 - Business use only (problem is enforcement and flexibility)
 - Alternative: business use only during working hours (not breaks)
 - Alternative: business and personal use – incidental, occasional personal use that does not interfere with employee's duties, that is not for monetary gain, does not conflict with company business or company policy.
 - No pornographic or other inappropriate websites used in workplace, which may give rise to harassment claims.
 - Company not liable for disclosure/misuse of personal information transmitted by employee over company technology (e.g. hacker steals personal bank data saved by employee on employee's computer.)
 - Employers should also inform employees that access to any Internet sites that are discriminatory or offensive is not allowed, and no employee should be permitted to post personal opinions on the Internet using the company's access, particularly if the

opinion is of a political or discriminatory nature

- Employer may access and monitor email and internet use at any time without notice
- Employer will keep copies of internet or email passwords, and that the existence of such passwords is not an assurance of the confidentiality of the communications

(ii) Discipline/termination policy for violations. As with all personnel policies, failure to enforce internet and email policies, or selective enforcement, may cause a waiver. Even worse, it could give rise to allegations of pretext in a retaliation, discrimination, or other employee claim. For example, if the employer has a strict business use only policy, but then knowingly permits employees to use computers for personal matters, and then fires a particular employee for such misuse, and the employee is a member of a protected class (e.g. race, gender, age, etc) then the employee may attempt to claim that policy was unfairly applied, or that it was a cover-up for discrimination.

Sample Policies

Disclaimer: These are generic sample policies only. They may not comply with current law in your jurisdiction. Consult with legal counsel before implementing personnel policies.

Company Computers

Company computers are essential to the business. Following are general guidelines regarding the use of Company computers:

1. Due to copyright infringement laws and the proliferation of computer viruses, employees are strictly prohibited from installing personal software on Company computers without authorization from the Office Manager or the President. Similarly, unless authorized, employees are prohibited from copying and installing Company software on personal or other non-Company computers.
2. All computer files and data in any form and on any electronic device owned by the Company or used for Company business are the property of the Company. The Company reserves the right to monitor and review information located on Company computers or other electronic devices used for business purposes at any time without advance notice. No Company employee, including management and the President, may alter or waive this policy unless it is done so in writing. Exercise of the right to monitor and review information may be invoked at any time irrespective of past and current Company practices. Therefore personal and/or private information should not be stored on Company computers. All passwords used in connection with computers, networks, or software must be disclosed to management. The use of passwords does not alter the right of the Company to monitor computer usage.
3. Management must authorize personal or off-duty use of Company computers.
4. Sending offensive, rude, obscene, sexually explicit, discriminatory, harassing, or other inappropriate electronic messages, or creating similar documents and files using Company computers is a serious violation of Company policy.
5. Playing computer games, accessing, or downloading non-job related materials from network services during work hours is a violation of Company policy.

Misuse of Company computers is a violation of Company policy and may result in disciplinary action, up to and including termination.

Internet Access

The Company has access to Internet services. Access to the Internet and other network services during working hours is limited to business use only. Employees may access the Internet or other network services for personal reasons during non-work hours and with prior authorization from the Office Manager or President of the Company. Internet usage is subject to monitoring at any time, without advance notice, by the Company to ensure compliance with this policy. At no time may the Company's Internet service be used for transmitting, retrieving, or storage of any communications of a discriminatory or harassing nature, or which is derogatory to any individual or group, or which is obscene or sexually explicit, or is of a defamatory or threatening nature, or for any other purpose which is illegal or against Company policy or contrary to the Company's interest. Downloading material not related to Company business from the Internet during business hours is a serious violation that may result in disciplinary action, up to and including termination.

Furthermore, employees are responsible for protecting Company information by not sharing sensitive or confidential information, including Company trade secrets, via the Internet.

Electronic Mail

Electronic mail on Company computers is Company property. Employees should not send electronic mail messages that they would not want management to read. Employees may not send electronic mail messages which are personal or private, or of a vulgar, hostile or threatening nature. Employees may not access the electronic mail messages of other employees without appropriate approval. Company management reserves the right to access and monitor electronic mail and other messages at anytime without employee notice or consent. Even where personal pass codes are used to access electronic mail, it should be understood that the President or an authorized representative may access electronic mail at anytime, with or without prior notice or consent. Therefore employees should refrain from including personal or private information in emails transmitted on Company computers, the network, or other Company property.

Voice Mail

The Company has installed a voice mail system on Company telephones for improved message delivery and storage. The Company voice mail system is owned and maintained by the Company, for business purposes only. Electronically transmitted messages on the Company voice mail system are not personal or confidential from the standpoint of the Company, and are subject to monitoring by authorized Company officials. Even if an employee uses a personal pass code to access voice mail, it should be understood that the President or an authorized representative may access electronic mail at anytime, with or without prior notice or consent.

Sending offensive, rude, discriminatory, harassing, or other unofficial electronic messages using Company voice mail is a serious violation of Company policy.

Searches and Monitoring

A. Purpose of the guideline

The Company believes that maintaining a workplace that is free of drugs, alcohol, and other harmful materials, including weapons, is vital to the health and safety of its employees and to the success of the Company's business. The Company also intends to protect against the unauthorized removal of Company property and to assure its access at all times to its property, equipment, records, documents, and files. Accordingly, the Company has established this guideline concerning inspections and searches on Company premises. This guideline applies to all Company employees.

B. Definitions

For the purposes of this guideline:

1. "Prohibited materials," includes but is not limited to firearms or other weapons; explosives, and/or hazardous materials or articles, illegal drugs or other controlled substances, drug-related paraphernalia, alcoholic beverages, and other prohibited materials on Company property that you are not authorized to have in your possession.
2. "Company property" includes all electronic or paper documents, records, software, data and files relating to the Company's business; and all equipment, hardware and other property of any kind, whether owned, leased, rented or used by the Company.
3. "Company premises" includes all premises and locations owned or leased by the Company or under its control, including parking lots, lockers and storage areas.

C. Inspections and Searches

1. Access to Company Property
 - a. In order to assure access at all times to Company property and because you may not always be available to produce Company property or information related to Company business that is properly in our possession when needed in the ordinary course of Company business, the Company reserves the right to conduct a routine inspection or search at any time for Company property on Company premises. In addition, the Company reserves the right to access at all times information and communications stored in Company computer files or in other electronic format, on Company disk-drives, and in employee voice mail boxes and electronic mail systems or other telecommunications/data devices.
 - b. Routine searches or inspections for Company property may include your office, desk, file cabinets, closet, lockers, computers, electronic devices, telecommunications/data devices or any other places where you may

place or store Company property or Company-related information, whether or not the places are protected by access codes and/or passwords. If personal keys or pass codes are used on Company property, a copy must be provided to the Office Manager.

- c. Because even a routine search for Company property might result in the discovery of your personal possessions, you are encouraged not to bring into the workplace any item of personal property that you do not want to reveal to the Company.

2. Inspections and Searches for Prohibited Materials

- a. Inspections or searches for prohibited materials on Company premises will be conducted whenever the Company has reasonable suspicion to believe that you may be in possession of such materials in violation of this Guideline or other Company policies.
- b.
- c. Inspections or searches for prohibited materials may include your office, desk, file cabinet, closet or any other places where you may place personal possessions, whether or not such places are locked. Inspections and searches for prohibited materials also may include your locker, Company vehicles and equipment and other Company enclosures, property or items.
- d.

D. Disciplinary Action

If you are found to be in possession of prohibited materials, in violation of this guideline and/or in violation of laws or work rules, or if you are found to have taken or used Company property in an unauthorized manner, you will be subject to discipline, up to and including termination regardless of the Company's reason for conducting the search or inspection.

If you refuse to cooperate during an inspection or search, you will not be forcibly detained or searched. You will be informed, however, that the Company will base any disciplinary decision on the information that is available, including your refusal to consent to the search as well as the information that gave rise to a reasonable suspicion that you were in possession of prohibited materials, if applicable, and that your failure or refusal to cooperate could deprive the Company of information that may clear you of suspicion. In addition, the Company reserves the right to take appropriate action to prevent the unauthorized removal from Company premises of Company property.

The information presented herein is intended as a brief overview of the law and are not intended to substitute as legal advice. Any questions or concerns regarding any statute or case law should be addressed to a licensed attorney. Copyright © 2008 by Barker Olmsted & Barnier, APLC. All rights reserved.