Legal Briefs – Workplace Privacy Participant Desk Reference

Legal Briefs
Employment Law Training Series

Workplace Privacy: Does it Really Exist?

Participant Desk Reference

Content input and review provided by:
T. Hensley "Ted" Williams, J.D., Co-Principal, The Williams Group, Des Moines, IA
Terri S. Miller, Department of Mental Health/Substance Abuse Services – Oklahoma
Internationally Certified Alcohol & Drug Counselor (ICADC)

Ms. Patricia Lamb, Employee Relations Consultant, Wells Fargo Mortgage, Des Moines, IA

TABLE OF CONTENTS

INTRODUCTION 1

PRE-ASSESSMENT 2

KEY CONCEPTS & DEFINITIONS 3

THE THREE ACTIONS 5

FAQ'S ABOUT WORKPLACE PRIVACY 6

FOR FURTHER INFORMATION 9

POST-ASSESSMENT 10

CERTIFICATION OF TRAINING 11

INTRODUCTION

This program is designed to help you gain a clearer understanding of an employee's rights to privacy and an employer's rights to protect property, information, and security.

Workplace Privacy: Does it Really Exist? provides answers to several of the most common questions managers struggle with concerning workplace privacy:

- Are individuals guaranteed the same rights to privacy within the workplace that they are entitled to at home?
- Should employees sign a consent form prior to any employer searches?
- Do I keep all records pertaining to an employee together, centralized in one location?
- After an investigation, should a full report of the incident be shared with the entire management team?

In addition, the program provides managers with three specific actions they can take to help ensure they keep themselves and your organization in compliance with the law.

The program is designed to cut through the legal jargon to provide clear and concise information in terms that everyone can understand.

PRE-ASSESSMENT

Instructions:

Please answer the following questions.

1. If someone wants to, they can track every keystroke on a particular computer.

   True or False

2. Consistency is very important. Preferential treatment for friends or employees with seniority could get you into legal trouble.

   True or False

3. If an employee is working on equipment or supplies that have been supplied by the company, then it is acceptable to monitor computers, phones, and day-to-day activities without notifying employees that you are doing so.

   True or False

4. Records of investigations and complaints should be kept separate from personnel files and kept as confidential as possible.

   True or False

5. If things are disappearing around your office and you think you know who is doing it, then it is perfectly acceptable to open up their desk or locker to look for missing items.

   True or False

6. Surveillance and monitoring of public restrooms is illegal.

   True or False

7. It is important to have specific procedures to go with your policies regarding workplace privacy so that you have a blueprint for action.

   True or False

8. When employers allow employees to purchase their own locks for lockers or storage units without providing the employers a key or combination – the employer is effectively waiving their rights of re-entry.

   True or False

9. Employees prior to any employer searches should sign a consent form.

   True or False

10. After an investigation of sexual harassment, a full report of the incident should be shared with the entire management team so that everyone can learn from the situation.

    True or False

KEY CONCEPTS & DEFINITIONS

Managing Expectations

While it is true that employees are working on equipment and supplies that have been purchased by the organization – unless you tell them otherwise, they come into the workplace with the same expectations for privacy that they enjoy in their own home. Depending on your organization's monitoring policies, this may be an unreasonable expectation. Therefore, it is important to make employees aware of what is private and what is not, and enforce these policies consistently.

Proprietary Material/ Trade Secrets

Many companies have proprietary material or trade secrets that they don't want shared with the public or their competition. So, they may monitor e-mail and voice mail to make sure that's not happening.

Productivity Measurement/Encourage Appropriate Usage

Computers or phones may be monitored for a couple of reasons:

- To measure productivity
- To make sure the resources are being used appropriately
- Inappropriate Internet surfing or downloading can create legal issues, bog down networks and cause other problems across an organization. Misuse of phones can drastically increase phone bills and dig into profit margins

Know and Support Your Policies

Review your policies and procedures regarding equipment use, confidential information, drug testing, and handling of employee records. Know where the information is outlined in the employee handbook. Emphasize policies at staff meetings. Understand what the policy provisions mean and what you need to do to support them consistently in your work area. Consistency is very important. Preferential treatment for friends or employees with seniority could leave you and your organization open to a discrimination lawsuit. Also, it is important to have procedures to go with your policies so that managers have a blueprint to follow for what appropriate actions they should take in the event of a workplace privacy issue.

Obtaining Employee Consent

As a manager, you should also make sure your employee has signed and dated an acknowledgement form that indicates they've received, read and understand the policies in the handbook. Please note: Employees do not have to agree with the policies—but they do have to acknowledge that they were communicated to them.

Protecting Confidentiality of Employee Records

Medical Records, Workers Compensation records and I-9 forms must be kept in separate, confidential files and NOT in with other employment records. If they are not, do what you need to do to fix it. Neglecting to take action to correct filing problems could open your organization up to a lawsuit. Also, make sure all personnel files are kept in one central, secure location – ideally in a Human Resources department. Don't leave files unsecured on your desk or out in your office while in your possession. Confidential information must be kept in an appropriate confidential file, preferably in a locked cabinet or office.

Protecting Confidentiality in an Investigation

The appropriate professional who knows the law should conduct any type of investigation based on the company's policies and procedures. A prompt, thorough investigation conducted with privacy issues in mind best meets the needs of the affected parties and the organization. If the complaint comes through you, work with the investigator to share all you know about the incident. Assist the investigator in keeping all meetings, interviews, and inquiries as confidential as possible. Results of the inquiry should only be shared after the investigation is complete and conclusions are final. And then, only those with an absolute need to know would receive the summary of the information.

Investigation Records

All records of the report, investigations, interviews, and conclusions should be kept in a confidential file, separate from the general personnel file. Putting investigation information in the wrong files can cause some real problems. Your HR professional will help you make sure the information is filed correctly so it's available for future reference.

NOTES

THE THREE ACTIONS

The three actions you can take to help make sure you're in compliance with workplace privacy issues are:

1. Know your organization's policies and procedures in regard to privacy, monitoring, drug testing, equipment use, and investigations, and enforce them consistently.

2. Communicate those policies clearly and completely. Make employees aware that e-mail, phone calls and voice mail, Internet and computer use, may all be monitored to ensure appropriate use.

3. Protect the confidentiality of employee records. Keep medical records, Worker's compensation records and I-9 forms in a secure location separate from the general personnel file. Also, record of investigations and complaints should be kept separate from personnel files and as confidential as possible.

FAQ'S ABOUT WORKPLACE PRIVACY

Q. What is the first step an organization should take if they decide to monitor their employees' phone, e-mail, or Internet usage?

A. An organization's first step is to define the policy and procedures. Let's face it; the best way to prevent a problem is to keep it from happening. Then an organization must take appropriate steps to ensure that managers and supervisors explain the monitoring policy to employees, they should have the employee sign a consent form acknowledging they understand the policy and consent to its implementation with respect to them personally. It is also helpful if during the communication, the organization takes the time to explain why the monitoring is taking place and what it will protect or prevent from happening. If your organization is going to monitor their employees, there should be a reasonable business purpose to support the action.

The other important aspect of communicating is doing so consistently. If you communicate to all current employees and don't add it to the new hire training, then the organization is being left wide open for potential hazards. However, if you cover all your current employees and all new employees in new hire training, then everyone has consistently been communicated to regarding the workplace privacy policy. Therefore, should a problem arise the next step should be very clear to the manager, organization, and the employee.

Q. If an employee is new to an organization and the organization has not clearly communicated the policy regarding workplace privacy, should the employee just assume there is no policy or should they inquire about the policy?

A. It is very important for an employee to take responsibility for complying with an organization's employment issues. Therefore, the employee should ask about the organization's policy. If the organization doesn't have a policy in place, the employee should think about this: if you are being paid by the organization to get a job done and you are doing something other than your job, then you are leaving yourself open to potential problems. While at work, an employee's best bet is to focus on their job duties.

Q. What type of information should a procedure on workplace privacy contain?

A. A procedure on workplace privacy should contain information regarding: Who will conduct a search? Will there be witnesses? How will it be documented? Where will the employee be? When will the police be called? Could the searches be random? Must there be reasonable suspicion? If company property is missing, will all employees' desks/lockers be searched?

Q. If an employee telecommutes, does the organization have the right to monitor them?

A. There is not a clear-cut answer here because the employee is technically at home. A good rule of thumb would be to ask yourself the following questions: Is the employee paid to work a set number of hours or during a specific time frame, for example 9 a.m. – 5 p.m.? If so, then during those hours an employer has the right to know what you are working on. Is the employee using company equipment? Is the employee logged onto a corporate website that will monitor activity? In order for a telecommuter to really maintain their privacy, their best bet would be to use their own personal computer for personal things and the business computer for work-related activities.

Q. Should all organizations have the same policy regarding workplace privacy?

A. No, although some policies may be similar in content, every organization needs to be conscious about having policies and procedures specific to their organizations' needs. Before an organization can monitor, drug test, or do a credit check on a potential employee, there should be a sound business reason for the organization to obtain this information. Also, the employee must have consented or acknowledged the monitoring or check.

Q. Do all states have to follow the federal guidelines regarding workplace privacy?

A. Yes. Federal guidelines take precedence over state guidelines, however, where state laws provide greater protection, organizations are usually subject to both. A state may choose to make their guidelines stricter than the federal guidelines as long as the state's guidelines don't conflict or negate federal guidelines. An organization may also choose to have their organizational policy and procedures even more detailed than the state guidelines as long as the guidelines do not conflict or negate the state or

federal guidelines. The most important thing for an organization to do is to communicate the policy and procedures consistently to all employees.

Q. My organization has an option in the e-mail software to mark a message confidential. Is the message really confidential?

A. Probably not. Most e-mail software has the capability to mark e-mail confidential or private. This does not mean that others cannot obtain access to the information or that a judge couldn't subpoena the information if applicable to a court case.

Q. Can my employer videotape me while I am working?

A. The answer depends on the type of work being monitored and if there is a specific business purpose for the monitoring. Federal law prohibits organizations from using video cameras to monitor any union meetings. State law may also limit the type of activities that can be monitored. For example, monitoring an employee locker room, or bathrooms may be forbidden.

FOR FURTHER INFORMATION

Here are some sources for additional information on workplace privacy.

Web Sites

The Privacy Foundation web page
http://www.theprivacyfoundation.org/workplace

Privacy Rights Clearinghouse
http://www.privacyrights.org

ScientificAmerican.com
http://www.sciam.com/

FindLaw.com labor and employment law links
http://www.guide.biz.findlaw.com

POST-ASSESSMENT

Instructions:

Please answer the following questions. Once you have completed the assessment and reviewed your answers with your facilitator, please sign and date the Certificate of Training on the next page. Then remove this page and turn it in to your facilitator.

1. If someone wants to, they can track every keystroke on a particular computer.

   True or False

2. Consistency is very important. Preferential treatment for friends or employees with seniority could get you into legal trouble.

   True or False

3. If an employee is working on equipment or supplies that have been supplied by the company, then it is acceptable to monitor computers, phones, and day-to-day activities without notifying employees that you are doing so.

   True or False

4. Records of investigations and complaints should be kept in one centralized location, separate from personnel files and kept as confidential as possible.

   True or False

5. If things are disappearing around your office and you think you know who is doing it, then it is perfectly acceptable to open up their desk or locker to look for missing items.

   True or False

6. Surveillance and monitoring of public restrooms is illegal.

   True or False

7. It is important to have specific procedures to go with your policies regarding workplace privacy so that you have a blueprint for action.

   True or False

8. When employers allow employees to purchase their own locks for lockers or storage units without providing the employers a key or combination – the employer is effectively waiving their rights of re-entry.

   True or False

9. Prior to any employer searches, employees should sign a consent form.

   True or False

10. After an investigation of sexual harassment, a full report of the incident should be shared with the entire management team so that everyone can learn from the situation.

    True or False

CERTIFICATE OF TRAINING

I understand the information presented in the course, ***Workplace Privacy: Does it Really Exist?*** I have also completed the post-assessment for this course and have reviewed the correct answers with my session facilitator or manager.

Employee's Signature Date

Facilitator's or Manager's Signature Date

This certification of training may be included in your personnel file as a record of having successfully completed this training.