**SHRM Employment Law**

Module 9: Employee Relations

Two people shaking hands

Description automatically generated with medium confidence



Time:  2 minutes

Running time: 2 minutes

**Objective**: Introduce the topic of Employee Relations.

**Description**:  Introduction to the topic and why it is important.

**Instructional Method**: Lecture/ice breaker

**Script:**

In the United States, we are very protective of our individual rights. We feel that our rights apply to us no matter where we are and what we are doing. However, some of our rights do not apply to the workplace like they do in a private home, in a public meeting, or on the street. This module will introduce the concepts of employee privacy in the workplace and how employers may and may not monitor employee activity both in and out of the workplace.

**Facilitator Notes:**

Add your name or any other information to this slide in the subtitle.

Graphical user interface, text, application

Description automatically generated

Time:  2 minutes

Running time: 4 minutes

**Objective**: Introduce the learning objectives.

**Description**: Show the objectives.  Answer any questions.

**Instructional Method**: Lecture

**Script**:

Here are the student objectives for this module:

* Define the key terms related to Employee Relations.
* Determine the appropriate laws to apply to given employment situations.
* Analyze employee rights concerning workplace privacy, private employee conversations, political and personal off-duty activities, and grooming and dress codes.
* Discuss reasonable expectations of privacy in the workplace.
* Examine issues related to using employee personal devices for work.

**Facilitator Notes:**

Use the objectives topics to create evaluation for the review.

Graphical user interface, text, application, email

Description automatically generated

Time:  6 minutes

Running time: 10 minutes

**Objective**: Define key terms for Employee Relations.

**Description**: Identify and define key terms for Employee Relations.

**Instructional Method**: Game

**Script**:

Let’s play a game to define some key terms used in the Employee Relations profession.

**Exercise**:  Key terms Game

**Note**: The winning group will have the most key terms listed correctly

7 Minutes

1. Put students into groups of 3 – 6
2. Have each group number a list from 1 – 12.
3. Read the definition of the term (note what number you read)
4. Have 1 student write the name (or number) of the term on their list.

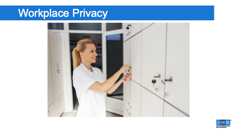
3 minutes

1. Give students the answers.
2. The team with the most is the winner.

**Facilitator Notes:**

**Key Terms**

1. **Appropriation of name or likeness-** The use of an employee’s name or photo without their permission.
2. **Audio surveillance**- Monitoring an employee’s phone conversations.
3. **BYOD policy**- A policy where an employer allows an employee to use their personal computers, phones, and other electronic devices for business purposes.
4. **Consent**- Agreement of the employee to the employer’s monitoring policy.
5. **Defamation**- Communicating information that might harm another party by damaging their reputation or discouraging others from associating with the party.
6. **Intrusion upon seclusion**- The intentional physical or other intrusion into the private business or space of another person.
7. **Invasion of privacy**- An intrusion upon another person’s reasonable expectation of privacy.
8. **Notice**- Notification to employees that they are being electronically monitored.
9. **Off-duty conduct**- The manner in which an employee conducts themselves while off-duty.
10. **Public disclosure of truthful but private facts**- The public sharing of private information that, while true, should remain private.
11. **Reasonable expectation of privacy**- The expectation that privacy is maintained in areas that should be private, such as restrooms and dressing rooms.
12. **Video surveillance**- Monitoring employees through the use of video recordings.



Time:  5 minutes

Running time: 15 minutes

**Objective**: Discuss reasonable expectations of privacy in the workplace.

**Description**: Ask questions to begin a discussion about this chapter.

**Instructional Method**: Lecture - Discussion

**Script**:

Workplace Privacy

* What rights do employees have to privacy at work?
* Can an employer monitor your computer and phone activity?
* What about searching your personal property, such as a purse, phone, or car?

Personal privacy issues in the workplace need more clarification than ever before in a world where personal devices are frequently used for business purposes. Let’s take a look at workplace privacy under the law.

Text

Description automatically generated

Time:  2 minutes

Running time: 17 minutes

**Objective**: Determine the appropriate laws to apply to given employment situations.

**Description**: Begin to discuss laws and how it relates to employee relations.

**Instructional Method**: Lecture

**Script**:

Although the right to privacy is not guaranteed expressly in the constitution, the Supreme Court has ruled that the details of the [First](https://www.law.cornell.edu/constitution/first_amendment), [Third](https://www.law.cornell.edu/constitution/third_amendment), [Fourth](https://www.law.cornell.edu/constitution/fourth_amendment), [Fifth](https://www.law.cornell.edu/constitution/fifth_amendment), and [Ninth](https://www.law.cornell.edu/constitution/ninth_amendment) Amendments already imply a right to privacy. The Supreme Court recognized the right to privacy in 1965 in the case [*Griswold v. Connecticut*](https://www.law.cornell.edu/supremecourt/text/381/479), a case about contraception, but the concept of the right to privacy bleeds over into the workplace in several ways.

The writers of the Constitution did not anticipate the need for privacy we would develop in our modern world of technology. Still, they did include the right to avoid unreasonable search and seizure (4th Amendment), freedom of religion and expression (1st Amendment), the right to avoid being forced to house members of the military in a private home (3rd Amendment), and the right to “life, liberty, or property” and requires “due process of law” (5th Amendment).

Diagram

Description automatically generated

Time:  15 minutes

Running time: 32 minutes

**Objective**: Determine the appropriate laws to apply to given employment situations.

**Description**: Have students use the Internet links to participate in the exercise.

**Instructional Method**: Lecture - Exercise

**Script**:

There are a number of laws (statutes) that help protect privacy rights in the workplace and provide guidance for employers about how they may use employees' private information.

**Exercise**: Laws and Employee Relations 10 minutes)

1. Break students into 6 groups (one for each law on the slide)
2. Have students use the Internet links to research the law.
3. Have students create a scenario that gives an example of how that law can be used in the workplace.

**Debrief** – Discussion (5 minutes)

* Have a spokes person for each group to describe their scenario to the class.

**Facilitator Notes:**

* Click on law in rectangle on slide to hyperlink to the site on the Internet explaining the law in more detail.

[**Electronic Communications Privacy Act (ECPA) of 1986**](https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285)

This law prohibits employers from intercepting oral, wire, and electronic communications of employees except for legitimate business purposes or when an employee consents to monitoring. An employer may not record a private conversation without first obtaining permission from an employee or without their knowledge unless the employees are using equipment owned by the employer (such as an instant messaging system on a corporate operating system), or if there are security issues that warrant monitoring.

[**Employee Polygraph Protection Act (EPPA) of 1988**](https://www.dol.gov/agencies/whd/polygraph)

A polygraph, or lie detector test, is designed to measure physiological changes against a baseline. The EPPA “prohibits most private employers from using lie detector tests, either for pre-employment screening or during the course of employment” ([EEOC.gov](https://www.dol.gov/agencies/whd/polygraph)). The exceptions to this rule are for “certain job applicants of security service firms (armored car, alarm, and guard) and or pharmaceutical manufacturers, distributors, and dispensers.

[**Fair Credit Reporting Act (FCRA) of 1970**](https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act)

The Fair Credit Reporting Act promotes fairness, accuracy, and information privacy and applies to employers in several ways. When employers run background checks or credit checks on applicants, they must rely on a third-party provider to obtain this information. However, before an employer can receive this information, several requirements must be met:

* Employers have to notify applicants or employees if they plan to use information from any type of consumer report when making employment decisions. This statement can’t simply be included on an application or job notice; it must be on a separate notification form.
* Applicants or employees must provide authorization for an employer to access their information from a consumer reporting agency.
* The employer cannot use the information in a discriminatory manner.
* The employer must notify the applicant or employee if they decide to take adverse action due to a consumer report and provide information about the reporting agency.
* The employer must provide the applicant or employee a copy of [A Summary of Your Rights Under the Fair Credit Reporting Act](https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.docx).

[**Health Insurance Portability and Accountability Act (HIPAA) of 1996**](https://www.cdc.gov/phlp/publications/topic/hipaa.html)

“The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient’s consent or knowledge” ([CDC.org](https://www.cdc.gov/phlp/publications/topic/hipaa.html)).

The law also outlines the rights and protections for employees and their dependents in group health plans, which employers frequently offer.

According to the [U.S. Department of Labor website](https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/our-activities/resource-center/fact-sheets/hipaa.pdf), HIPPA protects workers and their families by:

* Providing additional opportunities to enroll in group health plan coverage when they lose other health coverage, get married or add a new dependent.
* Prohibiting discrimination in enrollment and in premiums charged to employees and their dependents based on any health factors.
* Preserving the states’ role in regulating health insurance, including the states’ authority to provide greater protections than those available under Federal law.

**Nondiscrimination Prohibitions**

Employees and their family members cannot be denied eligibility or benefits based on certain "health factors". They also cannot be charged more than similarly situated individuals based on any health factors. “Health factors” include medical conditions, claims experience, and genetic information. HIPAA and the Affordable Care Act (ACA) also provide protections from impermissible discrimination based on a health factor in wellness programs related to group health plan coverage (such as those that encourage employees to work out, stop smoking or meet certain health standards such as a target cholesterol level).

Additionally, employers must further protect employee privacy by not placing protected health information in employee files to which managers or others may have access. Employees should have a separate file for any health-related information that an employer might gather for health insurance, vaccination information, Family Medical Leave documentation or anything related to protected health information.

[**National Labor Relations Act (NLRA) of 1935**](https://www.nlrb.gov/guidance/key-reference-materials/national-labor-relations-act)

As discussed in Module 1, the NLRA “Protects workplace democracy by providing employees at private-sector workplaces the fundamental right to seek better working conditions and designation of representation without fear of retaliation” (NLRB.gov).

This right to unionize gives employees the right to meet outside of working hours to discuss workplace issues without the restraint of having the employer present or interfering with the workday. When pre-union discussions occur, the right to privacy is important. Additionally, once a union is formed, employees have further rights to privacy under the terms of that contract.

[**Privacy Act of 1974**](https://www.justice.gov/opcl/privacy-act-1974)

According to the [U.S. Department of Justice website:](https://www.justice.gov/opcl/privacy-act-1974)

The [Privacy Act of 1974, as amended, 5 U.S.C. § 552a](https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf), establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual.

The Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register. The Privacy Act prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual, unless the disclosure is pursuant to one of twelve statutory exceptions. The Act also provides individuals with a means by which to seek access to and amendment of their records and sets forth various agency record-keeping requirements.

A picture containing text

Description automatically generated

Time: 4 minutes

Running time: 37 minutes

**Objective**: Discuss reasonable expectations of privacy in the workplace.

**Description**: Describe each claim and have students give an example.

**Instructional Method**: Lecture - Discussion

**Script**:

Employees can make claims of an employer invasion of privacy under several circumstances:

* Appropriation of name or likeness
* Public disclosure of truthful but private facts
* Defamation
* Intrusion upon seclusion

**Facilitator Notes:**

*Appropriation of Name or Likeness*

Employers may not use an employee’s name or image for advertising without the employee's express written permission. This includes website advertising or images. It’s simple enough to ask employees to sign a release if they want to be featured in advertising that the employer may benefit from, so employers should ensure they obtain permission before using employee images and names.

*Public Disclosure of Truthful but Private Facts*

Employers may not disclose private information about employees to others, even if the information is accurate. For example, an employer may share the information with a team that a team member will be out of the office for medical leave, but they may not disclose that the employee has contracted HIV and is undergoing treatment.

*Defamation*

Defamation is communicating information that might harm another party by damaging their reputation or discouraging others from associating with the party. For this reason, many employers do not provide reference information for former employers other than dates of employment. If an employer is going to provide a negative employment reference, they should be prepared to back that up with documentation in the event they are sued.

*Intrusion Upon Seclusion*

According to Rassas (2020),

This type of invasion could arise if an employer intentionally intrudes (physically or otherwise) upon the solitude or seclusion of another, or into a private affair or concern. Such conduct would result in liability for an employer if the intrusion would “be highly offensive to a reasonable person.” The intrusion might be related to a physical invasion of an individual’s personal space intended to be kept private, or it can refer to the use of one’s senses, with or without mechanical assistance, to overhear a conversation. Under this cause of action, potential liability attaches once the intrusion occurs rather than resulting from what is done with the information after it is uncovered.



Time:  3 minutes

Running time: 40 minutes

**Objective**: Discuss reasonable expectations of privacy in the workplace.

**Description**: Discuss employee’s reasonable expectation of privacy within the workplace.

**Instructional Method**: Lecture

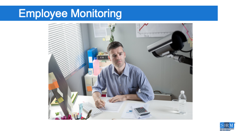
**Script**:

When courts become involved in employer privacy violation claims, they look at the employee’s reasonable expectation of privacy within that workplace.

There are two factors the courts consider:

1. Physical space- A private office or cubicle compared to a public breakroom or conference room.
2. Ownership- Does the employee own the area or property being searched or does the employer own it?

Additionally, the courts must determine how offensive the intrusion was to the employee. A hidden camera in the main work areas would likely not be considered an ***invasion of privacy***, while one in a restroom, breastfeeding room or locker room would be.



Time:  5 minutes

Running time: 45 minutes

**Objective**: Discuss reasonable expectations of privacy in the workplace.

**Description**: Discuss employee’s reasonable expectation of privacy within the workplace.

**Instructional Method**: Lecture - Discussion

**Script**:

Many employers monitor employees for any number of reasons including loss prevention, security, and productivity studies. In today’s society, most people are fairly accustomed to being on camera or having conversations recorded on a regular basis and don’t think much of it, so long as an employer doesn’t take it too far.

The ***reasonable expectation of privacy*** is that employers will only monitor public areas and not those intended to be private.

**Ask**: What would you consider to be an invasion of privacy in the workplace?

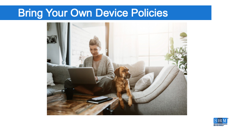
**Facilitator Notes:**

*Video Surveillance*

When using video to monitor employee activities, employers should be certain that the cameras are not located in areas like dressing rooms and restrooms, but instead are used in plain view of common areas where employees work. Some employers use the webcam on computers to monitor employees’ work habits

*Computer and Phone Surveillance*

Some employers use the webcam on computers to monitor employees’ work habits, as well as specialized software that can record everything down to individual keystrokes. Phone calls with customers are frequently recorded for quality control, and even interactions with co-workers can be recorded to use for documentation and training. Employers have every right to monitor the words and actions of employees during the workday and employees should be aware that they can be monitored at any time in many workplaces.



Time:  10 minutes

Running time: 55 minutes

**Objective**: Examine issues related to using employee personal devices for work.

**Description**: Have students pair up to debate the issues related to using employee personal devices for work.

**Instructional Method**: Lecture - Discussion/Debate

**Script**:

In our post-COVID world, we are realizing that many employers are now allowing employees to work from home using their personal computers, phones, and other equipment. While employers can certainly allow this, employees should be aware that they will bear some liability in ensuring that company information remains secure, and the use of personal devices for company business means that an employee’s personal devices can also be subpoenaed in the event of various types of lawsuits and investigations. Employers may not generally require an employee to use their own devices, but instead may offer it as a matter of convenience to the employee.

**Debate** (6 minutes)

1. Put students into groups of 4 (2 pair).
2. Have the pairs debate using personal computers instead of the company’s computers

**Debrief/Discussion** (4 minutes)

Summarize each group’s debates.

Timeline

Description automatically generated

Time:  5 minutes

Running time: 60 minutes

**Objective**: Determine the appropriate laws to apply to given employment situations.

**Description**: Explain the five rules in the law that specifically apply to employers involving Medical Privacy.

**Instructional Method**: Lecture

**Script**:

Medical Privacy

Employees are entitled to privacy concerning their medical records and information. Under the Health Information Portability and Accountability Act (HIPPA), employee medical information is considered protected information and is subject to special regulations. There are five rules in the law that specifically apply to employers:

**Facilitator Notes:**

The [PAYCHEX.COM](https://www.paychex.com/articles/employee-benefits/hipaa-rules-for-employers) website accurately outlines each of these:

HIPAA defines PHI broadly. However, some examples of PHI under HIPAA include demographic and contact information, such as a name, address, and a Social Security number that relates to an individual's past, present, or future health status. The definition of PHI also encompasses information related to payments made for the provision of health care.

HIPAA also specifically defines with whom protected health information can be shared. Primarily, covered entities and business associates can share PHI only in the following situations:

* With the person in question for treatment, billing, and healthcare operations;
* With descendants in the case of death;
* To a designated personal representative; or
* In response to a court order.

HIPAA rules require that covered entities provide notice regarding privacy practices and how PHI may be used or shared. The law is very specific regarding patient rights, what must be included, and when information must be presented.

Electronic Security Rule (45 CFR §164.308)

This rule requires [physical, technical, and administrative safeguards](https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html) be put into place to protect individuals' health information. The responsibility is placed on covered entities and their business associates to secure protected health information in electronic form. Organizations are expected to take the necessary steps to ensure privacy, protect against threats, ensure employee compliance, and protect against prohibited electronic uses or disclosures. Compliance is taken very seriously by regulators, with enforcement and penalties ranging up to $50,000 per violation and the potential of enforcement action in egregious cases.

Breach Notification Rule (45 CFR §§ 164.400-414)

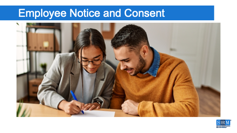
Under this rule, covered entities and business associates are required to report any breach that compromises an individual's protected health information. In the event of a breach, proper notification must be made to affected individuals, and copies of the notifications must be [submitted by the covered entity](https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html) to the secretary of the HHS.

Administrative Simplification Regulation (45 CFR 160, 45 CFR 162, and 45 CFR 164)

The Administrative Simplification provisions standardize the electronic exchange of healthcare information. National standards were set for electronic transactions, code sets, and unique identifiers. Employers must use their Employer Identification Number used for tax reporting as their identifier for all HIPAA transactions.

Omnibus Rule (45 CFR § 164.308, 164.312 and 164.316)

This rule expanded liability for business associates and instituted greater penalties for noncompliance. Additional rules prevent certain information from being shared about an employee's health plan when they pay for medical services out of pocket. Companies that may be defined as a business associate will need to [understand how their responsibilities have changed](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html) and make appropriate adjustments to their HIPAA policies or procedures.



Time:  2 minutes

Running time: 62 minutes

**Objective**: Discuss reasonable expectations of privacy in the workplace.

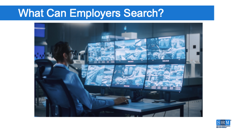
**Description**: Discuss employee notice and consent of monitoring.

**Instructional Method**: Lecture

**Script**:

If employers plan to monitor employees in any manner, employees should be notified of this intent and provide consent to it.

This can occur verbally during an interview by explaining the monitoring policy and asking the applicant if they will agree to the monitoring activity, followed by the receipt of a copy of the policy and a signed acknowledgment of the written policy outlining the activity during new hire orientation. Employers should also post signs in areas where monitoring occurs to remind employees that they are being monitored.



Time:  3 minutes

Running time: 65 minutes

**Objective**: Determine the appropriate laws to apply to given employment situations.

**Description**: Show the objectives.  Answer any questions.

**Instructional Method**: Lecture

**Script**:

What Can Employers Search?

Employers can reasonably search any property owned by them. This includes offices, cubicles, furniture, computers, phone systems, email systems, etc. However, there may also be an expectation of privacy for the employee because the employer has provided a space that can be secured by the employee without access by anyone else (such as a locker, or even an office).

**Facilitator Notes:**   
In cases of employer searches, the courts typically look at a couple of issues:

1. Is the search justified? Does the employer have reasonable (strong) suspicion that is work-related to conduct a search? For example, was an employee caught on security cameras putting money into their uniform pocket while operating a cash register?
2. What is the employee’s expectation of privacy? What is the culture, policy, and practice of the employer in regard to privacy? For example, is there a policy in the employee handbook that informs employees that their desks and lockers are subject to random searches?

An employer may not detain an employee to keep them from leaving the premises until their person and/or personal items are searched. If an employer believes an employee has stolen property in their personal vehicle or bags, they should contact local law enforcement for support.



Time:  10 minutes

Running time: 75 minutes

**Objective**: Analyze employee rights concerning workplace privacy, private employee conversations, political and personal off-duty activities, and grooming and dress codes.

**Description**: Have students discuss and analyze the areas of employee/employer rights on the slide.

**Instructional Method**: Lecture - Exercise

**Script**:

Employers may not prohibit employees from discussing the terms and conditions of their employment with other employees.

The [National Labor Relations Act](https://www.nlrb.gov/about-nlrb/rights-we-protect/your-rights/your-rights-to-discuss-wages) provides employees with the specific right to discuss matters concerning to wage, hours, working conditions, and more not only with co-workers, but also with others outside of the organization and the employer may not interfere with or retaliate against employees for doing so. The NLRA applies to most private employers.

**Exercise**: employee/employer rights

1. Break students into groups of 3-5
2. Have each group discuss and analyze employee rights using the subjects on the slide.
3. Have each group choose a spokesperson to summarize the group’s discussion.

**Facilitator Notes:**

Grooming and Dress Codes

Employers are free to set grooming and dress code standards at their organization, so long as those policies do not create disparate treatment or disparate impact against any protected employee.

If an employee’s religion, national origin, race, sex, disability, pregnancy, or other protected category indicates a need for an accommodation to the employer’s dress codes and grooming standards, the employer must make an accommodation.

For example, you might recall the 2015 Supreme Court Case [*EEOC v. Abercrombie & Fitch*](https://www.eeoc.gov/newsroom/abercrombie-resolves-religious-discrimination-case-following-supreme-court-ruling-favor). In this case, the employer refused to hire a Muslim applicant because of her religious practice of wearing a hijab. The company felt that the hijab didn’t fit with the “look” of their organization and so denied her employment.

According to [EEOC.gov](https://www.eeoc.gov/newsroom/abercrombie-resolves-religious-discrimination-case-following-supreme-court-ruling-favor):

In its June 1, 2015 decision, the Supreme Court held that an employer may not refuse to hire an applicant if the employer was motivated by avoiding the need to accommodate a religious practice. Such behavior violates the prohibition on religious discrimination contained in Title VII of the Civil Rights Act of 1964.

*Natural hair*

One area of potential discrimination centers on the topic of hairstyles, particularly those associated with African Americans and other minorities such as corn rows, braids, twists, locs, textured hair, and afros. Historically, these types of hairstyles have been banned by employers under their grooming policies, creating a disparate impact situation for those employees who have these types of hairstyles.

Seventeen states and Washington, DC have passed CROWN act laws. [CROWN stands for “Creating a Respectful and Open World for Natural Hair.”](https://www.govdocs.com/states-with-hair-discrimination-laws/) These laws protect the rights of minorities to wear their hair in styles suited to their race and culture regardless of employer policies.

Union Organization

We will discuss union organization more thoroughly in Module 12, but it bears mentioning that employers may not prohibit workplace conversations about unionizing activities. Employees may not shirk their work to discuss unionization, but they cannot be prohibited from discussing unionization.

Off-Duty Activities

While employees would like to think they can act however they like when not at work, employers do have the right to set some expectations for the off-duty conduct of their employees when that conduct could result in a negative impact to the employer. To do this, employers sometime use a morals clause in an employment contract that specifies particular behaviors that the employee will avoid while employed at the company.

Additionally, many employers include policy statements in employee handbooks concerning off-duty conduct of employees, especially in positions where public policy or perception can impact the business overall. For example, off-duty use of illegal drugs could impact the safety of the employee and others while at work; a high school teacher caught drinking with underage students is inappropriate and illegal, and a police officer Photoshopping images of coworkers onto pornographic images and sharing them online is an invasion of privacy and in violation of an oath to protect the public.

*Political Expressions, Activities, and Social Media*

What if your employee is involved in controversial off-duty activities such as a KKK rally? Employees are entitled to free speech, right? Yes. Employees are entitled to free speech outside the workplace. However, employers are also free to terminate employees under the “employment at-will” doctrine. You might recall an even in [August of 2017 when a driver plowed his car into a group of counterprotestors at a white nationalist and KKK rally in Charlottesville, Virginia.](https://www.michiganemploymentlawadvisor.com/human-resource-law-compliance/2582/)

Another white nationalist, [Cole White](https://www.washingtonpost.com/news/food/wp/2017/08/14/charlottesville-white-nationalist-demonstrator-fired-from-libertarian-hot-dog-shop/), who was attending the rally was photographed and the photos were published on Twitter as part of a campaign to identify racists through crowdsourcing. The man was employed at a hot dog shop in Berkeley, California and after multiple complaints and calls on the business owners to terminate the employee, he resigned. While the company did not terminate the employee for his political expressions, there is nothing to restrict them from doing so.

Can an employee complain about an employer on social media? Yes. As stated previously, the NLRA protects employee discussions about the terms of employment including hours, wages, shifts, supervisors, and working conditions. However, employers do have the right to terminate if employees are posting information that is untrue and causes harm to come to the company. Employees can be terminated for posting derogatory information about customers, clients, and vendors, as well as posts that are homophobic, anti-religious, sexist, or racist against other employees or the organization as a whole.

*Romantic Relationships between Coworkers*

Employers frequently have policies that regulate romantic relationships between coworkers, but the reality is that it is practically impossible to regulate relationships. However, an employer does have the right to terminate employees who violate this code of conduct, particularly if it interferes in the workplace. If an employer does discipline employees for romantic relationships in the workplace, it must do so fairly and equitably to all parties involved and employees.



Time: 5 minutes

Running time: 80 minutes

**Objective**: Determine the appropriate laws to apply to given employment situations.

**Description**: Students will review the material by answering the questions on the slide.

**Instructional Method**: Pair and share discussions, exercises, homework

**Script:** Let’s discuss different employment laws.

**Exercise**:

1. Pair students
2. Have students discuss and answer the questions on the slide.
3. Have students share their answers.

**Individual Exercise:**

1. Have each student write a one-page answer to question #2
2. Have students get into groups of 3-5 and discuss their answers
3. Have students share with the entire class (optional)

**Discussion Prompts**

1. Should employers be able to monitor employee social media accounts and require passwords to be provided? Why or why not? Are there some jobs that should require full disclosure?
2. How do you feel about computer monitoring in the workplace? Should employers use tracking software to ensure employees stay on task or is that an invasion of privacy?

**Case Law in the Spotlight**

* *EEOC v. Aviation Port Services, Inc*., Civil Action No. 1:18-cv-10909
* Ontario v. Quon, 560 U.S. 746 (2010)
* Frankhouser v. Clearfield County Career and Technology Center, Franklin Walk, Todd Jefferies, Gregory Paladina, and Doug McClelland (Case No. 3;18-cv-180)

**State Employment Law Focus**

* Does your state have laws that protect employee privacy? Check out this [link](https://www.getkisi.com/blog/state-employee-privacy-surveillance) and conduct further research to determine what laws, if any, apply to you!

**HR Skills Exercise**

* Research and develop a personnel policy suitable for inclusion in an employee handbook for the following:

1. Video surveillance
2. Email surveillance
3. Phone surveillance
4. BYOD policy

**Relevant Law:**

* Electronic Communications Privacy Act (ECPA)
* Employee Polygraph Protection Act (EPPA)
* Fair Credit Reporting Act (FCRA)
* Health Insurance Portability and Accountability Act (HIPAA)
* National Labor Relations Act (NLRA)
* Privacy Act of 1974

A picture containing text

Description automatically generated

Time:  10 minutes

Running time: 90 minutes

**Objective**: Review main points in this module.

**Description**:  Be sure that students have a fun way to remember the material.

**Instructional Method**: Game – Review

**Script**:

Let’s see how much we remember about this module.

**Facilitator Notes:**

Review Exercise:  Create a fun game to review the material.  Remember to use the objectives to measure learning:

* Define the key terms related to Employee Relations.
* Determine the appropriate laws to apply to given employment situations.
* Analyze employee rights concerning workplace privacy, private employee conversations, political and personal off-duty activities, and grooming and dress codes.
* Discuss reasonable expectations of privacy in the workplace.
* Examine issues related to using employee personal devices for work.
* Have each student submit a question on a piece of paper, crumple it up and toss it in a bucket (clean wastebasket), Instructor will then read them and give points to each team with the correct answer.
* Any game show – Family Feud, Jeopardy, $10,000 pyramid, Password, Tic Tac Toe
* Extra credit quizzes

There are many ways to review material virtually or in person.  Students can use their phones or computers to navigate to various online review websites.

A few are:

* Kahoot
* Quizlet