

HUMAN RESOURCE CONNECTION MONTHLY NEWSLETTER

VOLUME I ISSUE VI November 2008

Table of Contents

(Click on any title below to jump to that page)

Greetings.....	1
A Question of Employment Law: Preventing disruptive behavior in the workplace.....	2
EEOC UPDATE	3
Is the boss reading your e-mail?.....	4
Effective January 1, 2009, Massachusetts Regulations to Mandate Standards for Data Protection of Personal Information.....	6
Think Twice Before Delaying Reservist Reemployment.....	8
“I’ll Do It for Free!”	10

GREETINGS

Welcome to the all New...

Human Resource Connection Monthly Newsletter

Our aim is to reduce your HR headaches by providing the information and tools you need to make life easier! We will provide you with up to date Human Resource Information that will help you in your day to day operations.

If there is information that you are interested in seeing in this newsletter, please let us know by email at sgall@gallgall.com.

If you have a HR question email us and we can do a blind post (you will not be identified) in the newsletter and others can answer by email and we will do a blind post to you answer in the next months Newsletter.

Thank You, Steven E. Gall



Steven E. Gall
President
Bio

Gall & Gall Company, Inc. was founded in 1987, with corporate offices in Dayton, Ohio. We presently partner with customers in 19 foreign countries and all 50 states in the United States.

Gall & Gall was founded by **Beverly Gall**, Ohio’s first female Police Chief and the third female Police Chief in the nation and **Steven Gall** a former Police Officer with over 27 years in Human Resources.

Together, their background is varied and extensive in information gathering and Human Resources.

Gall & Gall has always been looked to as a leader in Employment Background Screening Services.

Contact Information:

E-Mail - sgall@gallgall.com
Toll Free 1-800-759-4255
www.gallgall.com

QUICK LINKS

(CLICK ON ANY LINK BELOW TO VISIT THE SITE)

SHRM (www.shrm.org) • **OHIO SHRM** (www.ohioshrm.org) • **MVHRA** (www.mvhra.org)

A Question of Employment Law: Preventing disruptive behavior in the workplace

By Jennifer L. Parent, Esq.

Louisa, a supervisor, contacts Henry, the human resources manager, because one of her employees, Dave, is making the other employees in the office uncomfortable. Louisa reports that Dave was recently divorced and has been going through a difficult time over the past year. He had expressed he was having financial problems that were causing him stress, and he was not happy with his last salary review. Louisa reports to Henry that while Dave did not seem to have engaged in any discriminatory harassment or physically aggressive conduct, he was irritable and aggressive in his speech. He also routinely talks about his gun collection and the number of guns he owns in general conversation. What should the company do?

Preventing disruptive, threatening and violent behavior in the workplace is a growing concern for employers. Anti-harassment policies typically cover only conduct for protected categories of discrimination (race, gender, sexual orientation, for example).

While conflict in the workplace is normal, employers should set and enforce clear standards of acceptable conduct.

As studies have shown, disruptive and hostile behavior results in reduced productivity of employees, poor morale, increased absenteeism, staff turnover, increased stress and anxiety, an unsafe work environment and potential legal costs.

Factors that may lead to incidents in the workplace are varied. An employee may be feeling rejected or overlooked in not receiving a desired promotion, transfer or raise, or may be experiencing anger due to the knowledge of a potential layoff. An employee may be experiencing psychological problems, under the influence of alcohol or drugs, or suffering from stress at home. These types of behaviors of concern may come from co-workers, customers or clients, or third parties outside the office.

Establishing a company misconduct policy not only sets a clear standard of acceptable conduct in the workplace, it also creates a protocol for handling threatening or violent behavior. Handling the situation

Training and company-wide publication of a misconduct policy reinforces the company's expectations of behavior and makes clear that disruptive, threatening and violent behavior will not be tolerated. Employees should be told that if they receive or overhear any threatening communications from an employee or outside third party to report it at once.

Employers also may consider prohibiting firearms (loaded or unloaded) and other weapons on the premises. Employee assistance programs also offer a cost-effective way of providing service to employees who need the support and guidance of a personal counselor for issues related to work, home or self and to the employer when it is faced with a volatile employee and not sure how to handle it. For example, EAP counselors can be available on-site when an employer is implementing a difficult lay off.

All reports of misconduct should be investigated carefully, promptly and to the fullest extent possible. Dealing with disruptive, non-threatening behavior, will involve a very different protocol from dealing with an immediate threat of violence. When appropriate, the company should meet with the individual and set clear expectations for improvement in job performance or in the relationship with co-workers or provide additional needed resources for outside help.

For specific threats of imminent violence, the course of action may include calling 911 (outside the sight or hearing of the individual), alerting others of the danger and getting people to safety as quickly as possible. Employees should not attempt to intervene physically or deal with a volatile situation themselves.

In Louisa's example, if it is determined that the situation is not a threat warranting immediate intervention under the policy, the company should investigate Louisa's report to determine specifics and to obtain examples of the conduct that gives co-employees concern.

Henry and Louisa should meet with Dave to discuss his behavior and the company's expectations of behavior in the workplace. If appropriate, the company may refer Dave to a counselor or an employee assistance program or another outside resource. At any stage, the company may seek assistance from a counselor or legal counsel. The company should also follow up to ensure that expectations are met and directed changes of the employee's behavior are made. All efforts and observations should be documented.

By instituting policies on workplace misconduct, companies can set clear standards of acceptable behavior and promote a safe work environment.

Jennifer Parent, a director in the Litigation Department of McLane, Graf, Raulerson & Middleton, Professional Association, can be reached at 603-628-1360 or Jennifer.parent@mclane.com.



EEOC UPDATE

EEOC Has Broad Power
To Subpoena Employer Records
By Christopher W. Olmsted

When the EEOC files an administrative charge of discrimination against an employer, it frequently will demand that company records be produced. If the company does not voluntarily comply, the EEOC may issue an administrative subpoena seeking to force production of the records.

The EEOC's power to obtain records is broad. The scope of its power is illustrated in a recent Ninth Circuit case titled *EEOC v. Federal Express*. In that case, after an employee filed a discrimination charge against FedEx, the EEOC opened an investigation and requested documents and information about electronically stored records. But then the employee obtained a right to sue letter and filed a private lawsuit. FedEx objected to producing records to the EEOC.

The court ordered FedEx to comply with the EEOC subpoena. The ruling is summarized below:

Requests After Right To Sue Allowed.

FedEx objected to the EEOC's record request because the charging employee had already received a right to sue letter and had filed a private lawsuit. The court held that the EEOC still had the right to obtain records.

The court read Title VII, the relevant regulations, and the EEOC's interpretation of those regulations to mean that: (1) the EEOC's investigative mandate is triggered by the filing of a valid charge; (2) the EEOC may bring its own action or may issue a right-to-sue notice to the charging party; and (3) even though the EEOC normally terminates the processing of the charge when it issues the right-to-sue notice, it can, under limited circumstances, continue to investigate the allegations in the charge, which includes the authority to subpoena information relevant to that charge.

Here, the aggrieved employee filed a charge alleging personal discrimination and discrimination against other similarly situated African Americans and Latinos. The EEOC, pursuant to Merritt's request, issued to him a right-to-sue notice. The EEOC decided, however, to continue investigating Merritt's charge because it involved a

possible policy or pattern of discrimination affecting others. The court found no legal authority to suggest that the EEOC exceeded its authority in doing so.

General Requests Allowed.

FedEx objected to the EEOC's request because it sought general employment files in order to help the EEOC draft future information requests, seeking evidence to a charge of systemic discrimination. The court held that the EEOC has the right to obtain general records even in the absence of a specific charge, in order to hunt for illegal conduct.

The court decided that broad requests regarding computer files are appropriate in the course of an investigation into policy or pattern discrimination. "The subpoena in this case asks FedEx only to identify any computerized files that it has or currently maintains. FedEx, the district court, and the EEOC all agree that that information is not necessarily relevant in an evidentiary sense. That is, the information sought is not itself evidence of discriminatory treatment in violation of Title VII. Rather, the information will help the EEOC craft additional information requests that may produce evidence of discriminatory treatment."

"[I]dentification of the computerized personnel information . . . is directly relevant to its investigation Such data permits the Commission to better focus its investigation. [T]his information will enable the EEOC to perform its investigative function by allowing it to frame more specific requests which will limit the possibility that irrelevant or unnecessary material will be produced for the EEOC to review. The efficient search for relevant information is imperative in a case like this, where the Commission must investigate not one or two claims against the company, but nearly two dozen. Without this means of locating pertinent data, both the EEOC and the employer could be overwhelmed by the sheer quantity of information needed to address each claim treated individually."

"To enable the EEOC to make informed decisions at

each stage of the enforcement process, Congress has conferred upon it a broad right of access to relevant evidence. Given this broad grant of power, it can hardly be said that the EEOC plainly lacks jurisdiction. Because Congress granted the EEOC the authority to investigate (and nothing in Title VII divests the EEOC of that authority when a charging party files suit) and because the evidence requested by the EEOC is relevant and material to the investigation, the district court did not err in enforcing the EEOC's administrative subpoena."

The Bottom Line

The bottom line is that the EEOC has broad power to obtain company records. The power is not without limitation. An employer has the right to redress in court to seek a narrowing of the subpoena. For this reason and others, it is appropriate to consult with legal counsel before responding to an EEOC request. However, as seen in the FedEx case, courts will generally permit the EEOC to obtain records relevant to the scope of its investigation.

This article 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. San Diego, California. All rights reserved. www.barkerolmsted.com

Is the boss reading your e-mail?

E-mail privacy is a myth, Sandra Gittlen explains, and what you're doing right now with e-mail, IM or blogs could get you fired.

Sandra Gittlen

Each day, it becomes more apparent that e-mail and instant messages are not private. Employers are worried about liability and lawsuits, so they're monitoring employee e-mail.

Their fears are not unfounded. The "Workplace E-mail, Instant Messaging & Blog Survey" by the American Management Association and the ePolicy Institute found that 24% of responding organizations have had employee e-mail subpoenaed, and 15% have gone to court to battle lawsuits triggered by employee e-mail.

On the other side, 26% of employers have terminated employees for e-mail misuse, and 2% have let employees go for misuse of IM. Even blogs are a cause of dismissal -- 2% of respondents reported firing workers for offensive content -- even if the blogs are not corporate based.

With employees encouraged to work longer and less-defined hours on company equipment, the lines between professional and personal use are becoming increasingly blurred. While organizations have gotten increasingly better about developing and communicating e-mail acceptable use policies, they are still lacking in addressing policies for IM and blogging.

Continued on Page 5
RETURN TO TABLE OF CONTENTS PAGE 4

The AMA found that 76% of the companies surveyed do have e-mail usage and content policies in place. That number drops significantly lower -- to 31% -- of employers that have IM policies in place. And only 9% have policies that address the use of blogs.

This lack of communications between employers and employees about expectations has set employees up for serious repercussions.

I recently discussed this changing landscape with Jeremy Gruber, legal director at the National Workrights Institute in Princeton, N.J.

What rights do employees have regarding privacy and corporate e-mail? What about using personal e-mail on a corporate computer or accessing corporate e-mail from a personal computer? Employees have virtually no privacy rights on their employer's corporate e-mail system. There is not even a hint of a balancing test involved.

Employers can monitor e-mail on their systems with total abandon and are not required to distinguish between personal and work-related messages. Indeed, an employer can monitor your e-mail messages if you are using the corporate system regardless of whether you are accessing the system from home or on the road, and can even access e-mail on personal accounts if it is accessed on the employer's server.

In fact, with the exceptions of Connecticut and Delaware, employers are not even legally required to tell their employees they are monitoring. State legislatures and Congress have completely abdicated their responsibility to regulate in this area.

What types of charges have you seen result in the dismissal of employees for using their e-mail? Employees have been dismissed for spending too much time on e-mail, sending "excessive" personal messages and for the content of their messages as well. Employees have been terminated for a single incident.

Often employer policies in this area are not very well developed, and employees are not aware that they have violated any rule. And since most employees are "at will" -- meaning they can be fired for any reason not protected by statute -- these minor violations can be an easy excuse for an employer to get rid of an employee for reasons that aren't easily justified.

Do you feel there is a catch-22 because employers want employees to be available 24/7 and equip them with corporate equipment/software? The traditional 9-to-5 static workplace doesn't exist anymore. Employees are more mobile than they have ever been before. A majority of today's workforce spends at least some time working outside the office with some regularity.

Employees are working longer hours than ever before, they are working from home, on weekends and even on vacations when they are emboldened enough to take them. Many are accessible by mobile devices at virtually any time during the day and night. The lines between home and work have been rapidly dissolving for some time.

The efficiencies and increased productivity that have resulted from this sea change have been entirely directed by employers for their benefit. While they are the driving force behind these fundamental 21st century workplace changes, their conception of workplace monitoring is rooted in 20th-century ideas that have little relation to the realities of the present workplace. An employee who is working in far excess of 40 hours a week and is constantly accessible remotely should be able to e-mail their child's pediatrician or engage in other necessary communications when they are in the office without fear of highly private content being made available to their employer.

What do you recommend that workers do regarding e-mail at work or on work equipment? Unfortunately, the only way to truly protect yourself from workplace monitoring as it currently exists is to only use communications devices that are exclusively under your control (not employer issued) and whose operation is in no way linked to the employer's equipment.

What are your feelings on acceptable use policies and their efficacy? Acceptable use policies go a long way toward recognizing the need for a reasonable amount of personal communication when at work. Still, many of these policies do not go far enough in that they continue to allow random monitoring without cause but simply set up a framework of rules that inform the employee of what types of behavior are acceptable or not. They may protect employees from inadvertently doing something that could affect their employment status but won't protect their privacy.

What is most egregious is that it doesn't have to be

this way. There may have been a time when monitoring technologies were too crude to adjust to a particular acceptable use policy but that is no longer the case.

Monitoring software is now highly customizable and if desired can be used in conjunction with an acceptable use policy that does not require random monitoring of personal communications. Even so, monitoring is often adopted as a supposedly easy solution to the far more difficult task of instituting and maintaining good management. It is not and will never be a good alternative, though.

Do you see the landscape changing in favor of the employee or the employer regarding e-mail privacy? There have been various attempts at the state and local level to pass legislation that would introduce some balance in this area. Where employers could meet reasonable business objectives and employees could maintain a comfortable level of privacy. As of yet, they have met with little success. There is no reason to believe the status quo will change anytime soon.

Can you point to any specific cases where an employee was dismissed for improper e-mail conduct? Alana Shoars was in charge of the Epson Torrance, Calif., plant e-mail system. Shoars assured Epson employees that their e-mail was private. She discovered later that her supervisor was reading all employee e-mail in the

Torrance plant. [Shoars v. Epson America]

Air force machinist Donald Thompson is placed under investigation [in 2004] by the Office of Special Counsel for forwarding an e-mail lampooning the president's qualifications. "To me, sending it was just an electronic version of water cooler chit chat," he said.

Heidi Arace and Norma Yetsko, two employees at the PNC Bank, were terminated after forwarding jokes on their company's e-mail. Such letters had been regularly sent in the past by fellow employees with the attention of the employer, and they had previously never enforced any monitoring policies.

More importantly, though, for every employee that has been reprimanded or terminated for an e-mail message, there are literally millions of employees whose personal communications are being read every day without their knowledge.

Sandra Gittlen is a freelance technology editor near Boston. Former events editor and writer at Network World, she developed and hosted the magazine's technology road shows. She is also the former managing editor of Network World's popular networking site, Fusion. She has won several industry awards for her reporting, including the American Society of Business Publication Editors' prestigious Gold Award. She can be reached at sgittlen@charter.net.

Effective January 1, 2009, Massachusetts Regulations to Mandate Standards for Data Protection of Personal Information

Massachusetts has issued sweeping regulations requiring companies to incorporate features into their security policies in an effort to combat identity theft. With the advent of the Digital Age and the near ubiquitous use of computers and the Internet in the U.S., a growing number of individuals regularly provide companies with their personal data—information that identifies a person such as a name, social security number, driver's license or financial account information. As the sharing of personal data has become somewhat commonplace for consumers and businesses, this information has also become the growing target of identity thieves, as evidenced by the occurrence of several large data breaches in recent years.

Most companies already take some precautions to protect and secure the personal data that they use and maintain.



Gauntlet Awards 1-800-541-2955
Crystal Awards, Acrylic Awards, Clocks, Plaques, Trophies, Pet I.D. Tags, Corporate Logo Apparel, Thank You Gifts, Holiday Gifts and Much More!
WWW.GAUNTLETAWARDS.COM

Recognizing the importance of this issue, almost all of the states, starting with California, have enacted some form of data breach notification law that require businesses to notify individuals if a breach of stored personal data occurs. These laws protect individuals by allowing them to take measures to limit the damages from a breach as well as reduce the risk of

identity theft by encouraging companies to bolster their security policies since notifications can be both costly and damaging to a company's reputation.

More recently, there has been a focus at both the state and federal level to enact legislation that goes beyond mere notification of data breaches. Some states, most recently Nevada, have enacted regulations or laws that mandate specific security requirements and impose legal liability on companies storing personal data who do not provide adequate security for the personal data they store.¹ However, most states that have passed or that are considering such laws often only require a reasonable level of security rather than a comprehensive set of security requirements for a company to comply with.

Starting in January 2009, however, companies dealing with Massachusetts' residents will now have a very specific set of security standards to guide and regulate their implementation of a data protection policy—201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth.² Recently released by the Massachusetts' Office of Consumer Affairs and Business Regulations, these regulations specify the types of personal data protected, what uses of this data by companies are covered by the regulations, and a set of standards and security requirements for companies to implement.

Scope of the regulations

To fall under these regulations, personal information must take on a very specific form. The information must be non-public data that contains a Massachusetts resident's first and last name or first initial with last name, in combination with any of the following:

- (1) Social Security number; or
- (2) driver's license number or state-issued identification card number; or
- (3) financial account number or credit card or debit card number (with or without any security code, access code or password).

The regulations apply in every circumstance irrespective of how a company obtains the information. They apply to companies that host consumer data of the types described above, but also to any company that employs

a Massachusetts resident, because employee records will always contain data that is personal information. If you are a company that owns, licenses, stores or maintains this type of data either electronically or on paper, then you must meet the minimum standards of protection set forth in these regulations.

What is required to comply?

Where a company is using personal information within the regulation's scope, that company must develop, implement, monitor and maintain a comprehensive, written information security program. This program must be reasonably consistent with industry standards and contain some administrative, technical, and physical safeguards. Although there is no bright line as to whether a company's security program will comply, since this depends on the nature of the business and the amount of personal information processed, the regulations do provide a list of features that every written information security program must contain. These features are as follows:

- (1) Designate at least one employee to maintain the program
- (2) Regularly assess risks to the security of stored personal information and mitigate any risks by improving the safeguards
- (3) Develop security policies for employees that access and transport personal data records and prevent terminated employees from access these records
- (4) Impose disciplinary measures for violations of a company's security program
- (5) If using third-party service providers, take reasonable steps—including obtaining written certification—to verify that they have an information security program that complies with these regulations
- (6) Limit the amount, time retention, and access of personal information to that reasonably necessary to accomplish the company's legitimate purpose

- (7) Regularly identify which records and storage media (including laptops) contain personal information
- (8) Adequately store and restrict physical access to personal information
- (9) Regularly monitor the effectiveness of the security program and review the scope of the security program at least annually
- (10) Document actions taken in response to security breaches

- (4) System monitoring for unauthorized use, firewall protection for Internet connections and use of up-to-date versions of software in the security systems.

What should you do?

Evaluate your existing IT security policies now. These regulations impose a level of protection of personal data never before seen in the U.S., but are frequently covered by existing IT security policies. Begin working with your outside counsel to determine the extent these new regulations will affect you and identify what steps you need to take to become in compliance when the regulations go into effect on January 1. Depending on what safeguards your company already has in place, extensive modifications and documentation may be necessary.

If you have any questions regarding this update or how the regulations discussed herein would affect your company, please contact one of the attorneys listed below:

- Alfred Browne - Boston, MA
- Jim Donato - San Francisco, CA
- Charles Schwab - Broomfield, CO
- Paul Schwartz - Broomfield, CO
- Miguel Vega - Boston, MA

www.cooley.com

Where a company using personal information within the regulation's scope also electronically stores or transmits that information, that company must also establish and maintain a security system covering its computers and must educate its employees on the proper use of such system. Features that the security system must contain are:

- (1) Secure user authentication protocols, such as control of user IDs and passwords
- (2) Secure access control measures to properly restrict access
- (3) Encryption of data that is sent over public networks, transmitted wirelessly, or stored on laptops or other portable devices

Think Twice Before Delaying Reservist Reemployment

By Steven Bernstein
(Labor Letter, November 2008)

As the war in Iraq drags on, employers continue to struggle with the legal challenges surrounding their reemployment obligations. The Uniformed Services Employment and Reemployment Rights Act (USERRA) sets a high bar when it comes to compliance, as illustrated by the fact that it remains the only federal workplace statute providing a built-in presumption in the plaintiff's favor. A police department in Nashville, Tennessee recently learned just how daunting the compliance challenge can be. *Petty v. Metropolitan Government of Nashville and Davidson County*.

Background

Sgt. Brian Petty had been supervising patrol officers in the fall of 2003, when he was called to active duty in Iraq. While overseas, he was accused of violating the Code of Military Justice by manufacturing wine and offering it to fellow service members. Following his arraignment, Petty accepted an offer to resign his commission "for the good of the Service," at which point all charges against him were dropped. He was subsequently discharged from service "under honorable conditions."

Following his discharge, Petty timely applied for reemployment, but the department advised him not to return until weeks later. The department began to suspect that he had concealed facts pertaining to his discharge from the military. In the interim, he was subjected to

return to work requirements applicable to other officers who sought return from extended leave of absence, including a medical exam, drug screen, and psychological debriefing.

Petty was also required to complete a questionnaire inquiring into his disciplinary history during military leave. Petty admitted that charges had been pressed against him, but neglected to disclose the substance of the allegations. He then attached a partial version of his form DD-214, a Department of Veterans Affairs document characterizing the basis for discharge from service.

Petty was subsequently reassigned to a desk position, while the circumstances surrounding his service discharge remained under investigation. Internal dishonesty charges were initially pursued, only to be withdrawn months later. At that point, the department obtained a complete copy of Petty's form DD-214, which described the basis for his discharge as "in lieu of trial by court-martial." Upon reviewing it, police officials concluded that Petty had altered his prior questionnaire to conceal this information.

Petty acknowledged that he failed to submit a complete copy of his DD-214. But he insisted that he was simply enlarging the form to make it more readable, thereby cutting off the information at issue. Finding his response unpersuasive, the department reassigned Petty to a position typically reserved for those officers facing internal discipline.

USERRA's Requirements Trump Department Procedures

In his USERRA lawsuit, Petty alleged that the department unlawfully delayed his reemployment and failed to restore him to his patrol sergeant's position, thereby discriminating against him by virtue of his military service. The department argued that it was merely adhering to uniform fitness for duty procedures promulgated by Nashville and the surrounding county. The lower court agreed and ruled in favor of the department. Petty appealed.

The U.S. Court of Appeals for the 6th Circuit referred to USERRA Section 4312, which guarantees a veteran's right to reemployment after a period of military service, as well as Section 4313, which prescribes the "elevator" position that must be offered to any returning service member. The Court made clear that in order to qualify for USERRA protection, one need only establish that he left the service under "honorable conditions," and that he subsequently made a timely application for reemployment, supported by documentation (such as a form DD-214) establishing that fact.

Although the department had argued that his form was incomplete, the Court sided with Petty's contention that it contained all information necessary to establish that he was qualified for reemployment under USERRA. The Court acknowledged that the department had an obligation to ensure that returning service members remain qualified to serve as police officers, but maintained that separation from service under "honorable conditions" is sufficient to qualify for statutory protection. The Court went on to note that USERRA prohibits adoption of a "policy plan or practice" that imposes additional prerequisites to one's statutory right to reemployment.

Absent unusual circumstances, USERRA requires the prompt reemployment of any individual so entitled. But in this particular case the department kept Petty out of work completely for three full weeks, and failed to subsequently return him to his regular duties. Under the circumstances, the Court concluded that the department lacked justification for delaying and limiting his return to work.

Lessons Learned

The upshot of this case is clear. Those employers who choose to delay reemployment from legally protected leaves of absence based upon unsubstantiated accusations or suspicions do so at their own peril. Generally speaking, the case also offers another subtle reminder of the substantial burden confronting employers that are forced to defend USERRA reemployment claims.

More broadly, it serves to reinforce the age-old proposition that supervisors may constitute an employer's first line of defense, but also its first basis for legal exposure in the absence of effective training. Much like other laws enforced by the Department of Labor (such as the Family and Medical Leave Act and the wage/hour laws) USERRA imposes a rigid set of standards that may run contrary to operational priorities, let alone common sense. Nonetheless, the courts continue to show a tendency toward enforcing its mandates to the letter.

Our advice? Arm all managers with a working knowledge of USERRA's requirements, so they can recognize a potential compliance issue at the front end of any return to work dispute. Preventive training in this area can help to insulate an organization from liability on the basis of an improper rejection or delay in reemployment that only festers with time, becoming a more difficult proposition months or even years later.

www.laborlawyers.com

“I’ll Do It for Free!”

By John Thompson

(Education Labor Letter, November/December 2008)

Many people are moved to volunteer their time to schools for religious, humanitarian, charitable, or other public-service reasons. No one wants to discourage these impulses, of course, but a school must be careful not to set itself up for a dispute over whether such a person is actually an employee for purposes of the federal Fair Labor Standards Act (FLSA). Being wrong about this could result in substantial exposure for things like minimum-wage and overtime payments, penalties for child-labor violations, and other liability.

What Does it Mean to “Volunteer”?

First, don't assume that the U.S. Labor Department or the courts will necessarily see volunteering time to a public school or school system in the same light as volunteers for private schools. For one thing, the FLSA itself provides that individuals who volunteer to perform services for a “public agency” (a term that typically includes government-operated schools) are not FLSA employees under certain circumstances. The statute contains no comparable exception that is available to private schools.

Also, DOL has said that its policy in all but “rare” situations is to limit volunteer status to people who perform activities for non-profit entities. Thus, a for-profit school might anticipate a high level of scrutiny should the status of a volunteer ever be in question.

DOL has recognized that, even outside of the public sector, there can be situations in which individuals may donate their services of a charitable or public-service nature in a non-employee capacity if they do so without expecting or receiving pay or benefits, on a truly voluntary basis, and without any coercion or intimidation. This general principle can be misunderstood to mean that non-employee volunteer relationships are easily and reliably established. That is not so.

For one thing, DOL maintains that employees may not volunteer to do things for their employer which are the same as or are similar or related to their normal duties; instead, it says, this is compensable worktime. DOL takes the same view regarding time an employee spends even in dissimilar services of a public or charitable nature, if this occurs at the employer's request, under its direction or control, or during the employee's normal working hours.

Some Key Factors

Other considerations can affect whether a person's efforts look more like volunteerism on one hand versus employment on the other. Among them are whether the activities:

- are truly undertaken for the individual's own personal, humanitarian, charitable, religious, or public-service motives;
- are of a kind typically associated with volunteer work;
- are less than a full-time occupation for the individual;
- do not involve replacing regular employees or impairing employment opportunities;
- are subject only to "nominal" or "minimal" control by the recipient of the person's efforts; and
- tend to occur at times suiting the individual's own convenience, whether by schedule or otherwise.

Schools should thoroughly evaluate volunteer relationships so that they can assess any possible exposure. The risk is probably highest as to people whom a school otherwise employs, especially if their volunteerism involves things that are the same as or resemble what they are paid to do. The danger is also likely to be substantial if what a volunteer does 1) either is or formerly was done by employees; 2) consists of things like general office work or other tasks which are an integral part of the school's "core" functions; or 3) are not of the sort ordinarily seen as charity, humanitarianism, or public service.

Compensating volunteers also creates a much greater chance that employment will be found. This does not necessarily preclude things such as reimbursing volunteers for mileage or sometimes providing a free cafeteria lunch. But the peril increases as the kind and amount of direct or in-kind payments begin to take on the appearance of wages.

Another potential problem is exercising close control over volunteers. Obviously, a school will want to manage things to maintain standards of safety, security, and propriety appropriate to the environment. On the other hand, the relationship takes on employment characteristics when there are rigorous dress and grooming standards, extensive and ongoing training is required, the volunteer must follow a strict schedule, there is a job description with detailed duties, volunteers are subject to employee-like kinds of discipline, and so on. If school administration believes that a high degree of control is necessary, then this might be a sign that the activities are not suitable for a volunteer relationship.

Summing It Up

These illustrations show that it can often be hard to decide whether a particular relationship is one of volunteerism or FLSA employment. In many "gray area" situations, no single factor will permit you to know for sure which way this question will be resolved if there is a challenge. Practically speaking, the organization to which a person provides services bears the risk of being wrong in classifying the activities as non-compensable volunteer ones. This might seem unfair given the uncertainty, but it reflects a philosophy that the FLSA is interpreted broadly to ensure that its requirements reach everyone it is intended to protect.

Finally, different federal laws or the laws of a state or another jurisdiction might apply stricter standards in this area. You should carefully evaluate volunteer relationships under every applicable law that is implicated by those arrangements. www.laborlawyers.com



Steven E. Gall, President
Gall & Gall Company, Inc.
The Information Source



Contact Information:

Phone: 937-264-4900

Fax: 937-264-4903

sgall@gallgall.com

Human Resource Management & Employment Law

Prior to entering the private sector, Steven worked in law enforcement and personnel administration for over twenty-seven years. He has dealt with employers and assisted them in resolving a wide variety of personnel problems and issues. Steven provides instruction and consulting to many Associations and Companies annually. His programs focus on all areas of HR Management.

Steven has conducted training sessions for Miami Valley Human Resource Association, Kentucky State Chapter of the Society of Human Resource Association, The National Apartment Association, The Florida State Apartment Association, The United States Department on Senior Care & Aging, The Cooperative State Research, Education, and Extension Service (CSREES) an agency within the U.S. Department of Agriculture as well as many other Associations and Companies Nationally. One of his areas of expertise is Employment Law, The Fair Credit Reporting Act, and Due Diligence in Employment Background Screening, Workplace Violence and other areas of Human Resources. Steven also speaks on Technology in today's workplace, "The Good, The Bad & The Ugly."

Professional Associations and Community Leadership Activities:

- SHRM Society of Human Resource Management – Professional Membership
- SHRM Ohio State Council – State District Director – West Central Ohio
- SHRM Chapter Miami Valley Human Resource Association, – Past President, Technology Director
- Miami Valley Military Affairs Association – Past President, Technology Director, Membership Chair
- Dayton Area Chamber of Commerce
- Huber Heights Chamber of Commerce
- Main Street Piqua
- Piqua Area Chamber of Commerce
- Tipp City Area Chamber of Commerce
- Trotwood Chamber of Commerce
- Troy Area Chamber of Commerce
- Vandalia-Butler Chamber of Commerce



Social Security Number Report, Employment Credit Report, County Criminal Records, Employment Reference Report, Drivers' License Record Search, Educational Credentials, Professional Certifications Reports, National Criminal Records, Statewide Criminal Records, US Patriot Act Search, Multi-state Sexual Predator and Violent Offender Search, Drug and Alcohol Screening and more!

www.gallgall.com 1-800-759-4255