

Welcome to the 2010 HR Connects

Sponsored by Human Resources

A copy of today's slides will be
available on our website at
www.uams.edu/ohr.

Welcome
HR Review

Hosea Long

AVC for Human Resources

Chief Human Resources Officer

Training and Events

Melissa Johnston

**Organizational Development
Manager**

Introduction of Keynote Speaker

Kathleen McComber

Senior Human Resources Director

Workplace Privacy Issues in the Digital Age

February 18, 2010

UNIVERSITY OF ARKANSAS FOR
MEDICAL SCIENCES
HUMAN RESOURCES GROUP



Allen C. Dobson
CROSS GUNTER WITHERSPOON &
GALCHUS, P.C.
500 President Clinton Avenue, Suite 200
Little Rock, AR 72201
(501) 371-9999
adobson@cgwg.com

New Technologies Bring New Challenges

- Blogs
- Social Networking
- Instant Messaging
- Email & Internet
- Cell Phones

What is a Blog?

- An online journal
- Can contain anything the author wishes to publish
- Risks:
 - Invasion of Privacy
 - Defamation
 - Sexual Harassment
 - Productivity drains
 - Negative Public Relations

Blog Risks

- Example:
 - Microsoft employee hired in part because of his personal blog.
 - After joining Microsoft, he had to self-censor his blogs, because his attacks on industry figures would now come off as Microsoft's attacks, not his own.

Blog Risks

- Fear of “sanctioning” blogs
 - May be held accountable for employee posts
- Fear of maintaining a monitoring policy
 - Knowledge of discriminatory or harassing content may expose employer to liability
 - Employer’s have not yet been held liable for employee blog content
 - However, liability HAS been imposed for employee email & internet conduct.

Discipline Actions for Employee Blogging

- National Labor Relations Act (NLRA)
 - Does not seem to prohibit employees termination/discipline for “acts of disloyalty,” such as blog postings criticizing an employer’s products.

Discipline Actions for Employee Blogging

- Employees have been terminated for the content of their personal, “home-based” blogs . . .
 - . . . however, NLRA prohibits disciplinary action for “protected activity”
 - criticism of terms/conditions of employment (protected)
 - Emails containing this info fall under NLRA protection, it is likely that blogs do too

Corporate Blogs

- Companies may have their own blogs
 - Accessible to employees or public
- Fewer than 2% of companies review blog entries and/or third party comments before they are posted.

Corporate Blogs: Risks

- Defamation and privacy torts
- Disclosure of Confidential Information
- Trade Secrets
- Securities Fraud
- Intellectual Property Infringement
- Discovery
- Loss of Business Due to Bloggers
- Harassment Claims
- Trade Libel
- Employment Issues
- User Privacy

What is Twitter?

- A free blogging service that lets users post short answers, known as “tweets,” to the question: What are you doing?
- Tweets create the same risk issues that blogs in general create; however, because they are instantaneous messages, they are generally not well thought out. This creates more potential for poor judgment.

Social Networking

- Facebook, MySpace, etc.
 - Websites providing an interactive, user-submitted network of individuals.
 - Public personal profiles, blogs, photos, music and videos

Social Networking

- Fastest growing segment of websites
 - Facebook and MySpace each attract approximately 115 million unique visitors each month.
 - Facebook statistics claim 3 billion minutes are spent on Facebook each day (worldwide)

Social Networking

- Employer Liability
 - In 2009 the Federal Trade Commission updated its advertising regulations for the first time in nearly 20 years. Effective in 2009, advertisers must disclose their relationships with companies when promoting a product or company in their blogs or other social media.
 - Employers could be liable for what employees say about products or services provided the employer if the statement could mislead consumers.
 - Employers should require employees to disclose the employment relationship when endorsing a product in their personal blog or social network account.

Social Networking

- Employee Recruitment
 - Employers are increasingly making employment decisions based on information obtained on social networking sites
 - These online searches can reveal a lot of information not attainable through customary searches: risqué pictures, pictures of drug use or heavy alcohol use, poor writing skills, and radical political positions

Social Networking

- Risks
 - Inaccurate Information
 - Employment Discrimination
 - Fair Credit Reporting Act
 - Terms of Service Violations

What is Instant Messaging?

- Free software download which enables people to type to each other and respond instantly
 - “Instant email”
- Risks
 - Inappropriate content in instant messages
 - Pornographic chat, jokes, etc.
 - Employees can send attachments
 - Easy disclosure of confidential information

What is Instant Messaging?

- Vulnerability to viruses and hackers
 - Unlike other electronic communications, instant messages are generally unprotected
- Employers with knowledge can be held responsible for content

Instant Messaging: Risks

- Instant Messages create a written record
 - Can be used for evidence
 - Can be subpoenaed in a lawsuit or administrative proceeding
- Employers may be exposed to liability for failing to implement policies to retain instant messages
- Instant Messaging is considered a form of email and should be governed by similar policies

Email & Internet

- Expose employers to a wide variety of risks
 - Downloading is a major issue
 - Offensive Material
 - Virus-infected files
 - Employers may be held liable for discrimination claims relating to downloaded material
 - Employees may claim downloaded material is degrading or offensive, or that it creates a “hostile working environment”

Email & Internet

- Employer may be held liable for statements made by employees that seem to speak on behalf of the employer
- Downloaded material may cause security or confidentiality breaches
 - Online connections expose this material to hackers

Email & Internet: Metadata

- Metadata is imbedded information in electronic documents
- It can expose confidential information, revealing:
 - File Type
 - Creation and Edit Dates
 - Authorship
 - Edit History

Email & Internet: Metadata

- Microsoft Word and Corel WordPerfect have features for viewing previous versions, tracking changes, and adding comments to a document
- If not disabled, this allows the recipient of the document to uncover information the sender did not intend to reveal

Cell Phones

- In ever-increasing numbers, employees are given cell phones or personal data assistants such as the Blackberry, so that they can work at any time, in any place

Cell Phone Risks

- Using cell phones while driving:
 - Employers spend approximately \$16,500 for each on-the-job employee auto accident
 - That amount rises to \$76,000 when injuries are involved

Cell Phone Risks

- Arkansas Act 247: “To Prohibit a Driver Under Eighteen (18) Years of Age From Operating a Motor Vehicle While Using a Cellular Telephone Device”
 - Applies to all violations committed on or after October 1, 2009.

Cell Phone Risks

- Arkansas Act 247: “To Require a Driver of a Motor Vehicle to Use a Hands-Free Wireless Telephone Device While Driving on a Public Highway”

Cell Phone Risks

- Arkansas Act 181: “Paul’s Law: To Prohibit Drivers of Motor Vehicles from Using Handheld Wireless Telephones to Engage in Text Messaging”
 - Applies to all violations on or after October 1, 2009.

Cell Phone Risks

- Camera phone use in the workplace:
 - Risk of confidential information disclosure
 - Risk of harassment from unauthorized pictures that are taken without consent and handled in an inappropriate manner.

Employee Expectations of Privacy

Employee Expectations of Privacy

- Contrary to what many employees assume, private-sector employees have almost no constitutional right to workplace privacy, and public-sector employee privacy rights are limited.
- Workplace computers and everything on them almost always belong to the employer. Employees may NOT assume that the contents of their workplace computer are private.

Employee Expectations of Privacy

- The 9th Circuit Court of Appeals recently provided a reminder that, for purposes of the 4th Amendment, an employee of a private company that has *an announced policy* of monitoring employees' use of computers, including the internet, has no reasonable expectation of privacy in the contents of his or her company-supplied computer.

Employee Expectations of Privacy

- With respect to an employee of a *public institution*, the 9th Circuit Court of Appeals recently found that the 4th Amendment *does protect* an employee's privacy in some cases.
- Specifically, an employee of a private company that has *an announced policy* of monitoring employees' use of computers, including the internet, has no reasonable expectation of privacy in the contents of his or her company-supplied computer.

Employee Expectations of Privacy

- New Jersey: Employee should not expect privacy on workplace computer
 - N.J. employer searched workplace computers and discovered employee has stolen thousands of dollars from the company.

Employee Expectations of Privacy

- The employee claimed the search was unjustified because it violated his right to privacy
 - He argued that he had a right to expect his personal information stored on computers to remain private because he kept them in a private office and had his own private password.
- The court disagreed.

Employee Expectations of Privacy

- Monitoring:
 - Employees may argue that monitoring technology use violates privacy rights
 - Employees may bring suit under the Electronic Communications Privacy Act (ECPA)
 - Title I of ECPA: Wiretap Act
 - Prohibits employers from “intentionally” intercepting certain communications, including email

Employee Expectations of Privacy

- Courts generally hold that liability only attaches if an employer intercepts an email “contemporaneously” with its transmission
 - Email retrieved from storage do not violate the ECPA
- ECPA has not extensively been applied to new technologies

Employee Expectations of Privacy

- Another New Jersey case:
 - *Stengart v. Loving Care Agency* (2009)
- Former employee, an executive with company, used company-provided computer to access personal email in order to email employee's attorney about filing suit against employer.
- Employer used image of emails found on computer during discovery phase of suit against employer.

Employee Expectations of Privacy

– *Stengart* Court found that:

- Because employer's computer use policy allowed for occasional personal use, the employer could not claim ownership or rights to all of the documents that the employee created and accessed even though the computer use policy stated that the employer could.
- Employees retain some privacy and ownership rights even if the employee signs an employer policy that states that the employee will not retain such rights.
 - Some of these rights include:
 - » Attorney-client privilege
 - » Information from bank accounts, medical records, income tax returns, and phone records.
 - » Other confidential matters

Employee Expectations of Privacy

- The employer failed to keep clear records of very important documents and was unable to
 - Make clear what computer use policy was in effect
 - » The court counted five possible policies!
 - Obtain or show that it had obtained an acknowledgement from the plaintiff that she understood and would comply with the computer use policy
 - » It was unclear whether the employer provided the policy to the plaintiff.
 - Show whether the computer use policy applied to executives such as the plaintiff.
 - » The plaintiff testified that she did not believe that the policy applied to her, and another executive testified similarly.

Employee Expectations of Privacy

- Lessons from *Stengart*:
 - Create a computer use policy that:
 - Warns the employee that the employer retains ownership and other rights to whatever documents the employee creates or accesses
 - » Be prepared for the court to place limits on these rights and have a fall back plan if the court does not enforce all aspects of the policy
 - Consider implementing a “no personal use” policy
 - » Allowing some personal use may make ownership claims difficult
 - ALWAYS
 - » Get an acknowledgment of the current policy
 - » Document, Document, Document
 - » . . . AND DON'T LOSE the documents!

Employer Rights

Technology Policies Protect Employers

- Employers may be able to reduce the risk of liability for workplace technology use by keeping tabs on how employees are using their computers, email and other electronic communications at work.

Technology Policies Protect Employers

- Companies should enact a comprehensive internet, email, and phone-use policy which addresses the proper use of the systems and the potential for the monitoring of electronic communications.
 - Stay on top of how employer's duties and obligations are affected by new technology.
 - New online technologies and trends in use by employees must be addressed by broad policies.

Technology Policies

- Make sure technology policies address the following issues:
 - Monitoring of employees – when & how
 - Company property – identify & define broadly
 - What is appropriate use of company property?
 - What is prohibited use of company property?
 - What personal use of company property is allowed?
 - “For business only” purposes are difficult to enforce.

Technology Policies

- Make sure technology policies address the following issues:
 - Electronic devices used to communicate or transmit information.
 - Unauthorized internal or external communication of confidential or proprietary information should be prohibited.
 - Expectations of privacy
 - Make it clear that employees should expect none.

Technology Policies

- Don't assume employees have knowledge of what content and conduct is appropriate
 - Make policies CLEAR. It is easier to discipline for improper use.

Technology Policies

- Draft policies carefully to insure against discrimination or harassment cases.
 - Inappropriate, harassing, offensive, defamatory or discriminatory content in any electronic communication, personal or business-related should be prohibited.
- Prohibit specific actions, such as sending offensive materials, or storing or accessing them.

Technology Policies

- Companies should distribute copies of the policy to all employees and require written acknowledgement and consent to the policy.
 - Obtain consent prior to monitoring.
 - Always insure employees have been directly informed of Company policy.
 - Place a message on your computer system’s “splash screen” about privacy rights.

Technology Policies

- Employees need periodic reminders of the applicable policies and the consequences of violations.

Developing Your Policies

New Technology: Developing Policies

- Regarding employee use of internet publishers, such as blogs, Twitter, and social networks:
 - Prohibit employees from revealing confidential information.
 - Prohibit negative comments about employer's product(s).
 - Require employees to include a disclosure when blogging, Twittering, etc. about the company or the company's products or services.

New Technology: Developing Policies

- Prohibit blogging using company resources or while on company business
- Prohibit defamatory or racially or sexually offensive material or remarks about other co-workers.

Corporate Blogs: Developing Policies

- Establish terms of use.
- Post appropriate disclaimers limiting the company's liability for third-party statements and other claims.
- Include provision for regularly monitoring the corporate blog.
- Provide for archiving blog content.

Instant Messaging: Developing Policies

- Create a policy that:
 - Maintains the employer's right to monitor instant messages.
 - Addresses the appropriate use of instant messaging software.
 - Addresses whether it is allowed at all.
- Prohibit employees from downloading instant messaging software.
- Develop policies for retaining and retrieving instant messaging records.

Email & Internet: Developing Policies

- Employees have a heightened sense of privacy with personal email accounts.
 - Remedy this by blocking software
 - Prevent employees from accessing personal accounts altogether.
 - 28% of companies use blocking software to prevent employees from accessing personal accounts.

Email & Internet: Developing Policies

- Flagging Software
 - Screen employee emails for offensive or confidential information.
 - Software scans for specific words.
 - Sends a “flagged” email to the person responsible for enforcing company policy.

Email & Internet: Employer Duty

- Monitoring:
 - 2005: Supreme Court of New Jersey ruled that if employer has *reason to know* that an employee is accessing child pornography on workplace computers, employer has a *legal duty* to monitor and investigate the computers.
 - Employer MUST inform law enforcement of the employee's activities.
 - Employer MUST take action to prevent such further conduct by the employee.

Cell Phones: Developing Policies

- Possible Cell Phone Policies:
 - Banning all cell phone use while driving on company business.
 - Prohibiting cell phone use in areas that contain confidential information.
 - Limit cell phone use in areas where phones could be used to harass.
 - Ban ALL cell phone use while at work.

“Technology Tools”

- Use emerging technology to your advantage!
- Technology tools assist employers in managing the use and misuse of emerging technology in the workplace.
- Monitoring, flagging, and blocking software lessen employer’s risk of security breaches and litigation.

Announcements
Question and Answer Session
Conclusion

www.uams.edu/ohr

please complete satisfaction survey

Teletha Leonard
Director of Employee Services