EMPLOYEE PRIVACY ISSUES IN THE SOCIAL MEDIA WORLD

June 27-30, 2012

Youndy C. Cook
University of Central Florida
Orlando, Florida

Traditional employer surveillance of the workplace and employees is a familiar concept. It generally consists of physical surveillance of an employee (such as having an investigator follow an employee for a workers compensation claim investigation) or video and/or audio surveillance within the workplace (often installed for security and anti-theft purposes, or for performance monitoring). Electronic workplace monitoring may be less familiar and can take various forms. Employers can, and many do, monitor all Internet usage and email traffic on the employer-operated system, or block access to certain categories of websites. Some employers also monitor off-duty social networking for information directly related to the employer. Although there are no hard statistics, anecdotal evidence suggests that tracking of employees and operations through mobile devices (GPS systems in mobile phones; iPad or other tablet tracking) and vehicles (GPS devices or linked navigation systems) is becoming more common.

The potential benefits to an employer from electronic workplace monitoring must be balanced against the potential legal issues or practical pitfalls of gathering such information. This paper discusses the advantages and disadvantages stemming from electronic monitoring and presents policy and other considerations for institutions of higher education to consider.

I. Employer Monitoring of Workplace/Employees

There are many things about electronic workplace monitoring that make sense. An employer obviously does not wish to see its workforce spending their days playing World of Warcraft or shopping eBay auctions. Nor does an employer want to see an employee disparaging it on line or in email, or transferring confidential information to outside sources. If a piece of software can easily address these issues by identifying who in the workforce is doing those things, an employer may naturally consider installing that software. A monitoring program can reduce inventory shrinkage, especially if employees know about it. A system of tracking employer-owned vehicles can reduce wear and tear on vehicles (by enforcing designated routes – and traffic laws) and ensure that employees are where they are supposed to be when they are supposed to be there. If your campus operates a shuttle system or a share ride system, a tracking system on the vehicles (or in the radios assigned to drivers) can improve on-time operation and offer an additional safety factor.

Tracking software and other monitoring products are readily available. Various companies promote software and products that monitor employee use of work-provided Internet access, cell phones, and vehicles. An employer that issues mobile phones to its employees has various options to track the position and use of those mobile phones. The same applies to vehicles. One AT&T Mobile Asset Solutions advertisement calls the use of their GPS-based

product "the bell on the cat." I leave it to the reader to ponder what the employees call it. Some products have default security settings that allow device tracking – these settings are designed to recover and/or wipe clean the device in the event of a theft, but the technology can be put to other purposes.

A basic search reveals an array of websites offering products that monitor and track. One site offers software for mobile phones called StealthGenie. The software can, among other things: record or intercept calls on the phone; log call history; monitor email and text messages from the phone; perform real time geo location tracking; give the user a notification if the device leaves a certain predetermined area ("GeoFencing"); activate the microphone to record or listen to surroundings; and view contacts and other data saved to the device. SpectorSoft offers products to monitor all user and user group activity on all network machines; products to conduct focused investigations with software that will record all email/webmail, keystrokes, chat/instant messages, internet activity, file transfers from a particular machine; and products to capture mobile phone activity. Other products that perform some or all of these same functions include: MobiStealth, ExtraSpy Employee Monitor, Easytime, ActivTrak, and Zecurion. [Very little or no legal analysis of these products is available on these sites. The use of some of these products, or some aspects of them, conceivably could violate federal or state law, such as wiretap laws.]

If the idea of monitoring and tracking makes sense, and products are readily available to do it, why don't all employers do it? They don't, because there are legal issues and practical considerations that may make such programs, depending on the circumstances of the workplace, not worth the effort. For example, some may suspect or know that employees in their workplace would find such monitoring unacceptable. This may be especially true in higher education, which tends to have a tradition of self-supervision for faculty and quasi-faculty ranks.

II. Legal Issues

A. For the Public Sector – Fourth Amendment Issues

For those employers in the public sector, as many universities and colleges are, the Fourth Amendment must be considered in any decision to monitor/track employee. The seminal case on public sector workplace searches is *O'Connor v. Ortega*, 480 U.S. 709 (1987), which yielded a plurality opinion. There, the Court focused on whether the employee had a reasonable expectation of privacy in the workplace given the 'operational realities' and, if so, the extent of that expectation and whether the employer's intrusion on that expectation was reasonable under the circumstances. While the case dealt with a physical search of an office and the contents of the office, the same legal analysis stands. A more recent case, *City of Ontario, California v. Quon*, 130 S.Ct. 2619 (2010), focused on more modern technology (pager transmissions), but did not recede from the operational realities and reasonableness tests of the *O'Connor* case. In *Quon*, the City was concerned by the extraordinary pager use by its employee and reviewed the transmissions to determine how many were work-related versus personal. Mr. Quon sued the City alleging a Fourth Amendment violation of his privacy. The Court declined to explore the operational realities analysis with a holding that the City's search was reasonable and necessary for a non-investigatory work purpose.

A recent Supreme Court case, *United States v. Jones*, 132 S.Ct. 945 (2012), held that police placement of a tracking device on a personal vehicle and the monitoring of that tracking device for 28 days was a search. Because the police did not obtain a warrant for this search, and because the Court did not consider whether the search was reasonable (the issue was not raised below), the Court therefore reversed the drug trafficking conviction obtained, in large part, using the evidence obtained during the search. Commentators have noted that the Court did not conclude (in fact, not one Justice concluded) that the mere intrusion into the car via the placement of a GPS tracking device was a search. Four Justices suggested that short-term monitoring of such a device would also not be a search. Thus, this case, while highly intriguing, is not a statement that warrantless GPS tracking is a Fourth Amendment violation.

The best way to avoid these issues is to clarify the reasonable expectation of privacy for employees by explaining (in policy or written agreements with employees) acceptable personal use of employer-provided equipment and the scope of any searching, monitoring, or tracking that will be done by the employer, and then to monitor or track only within the scope of that clear policy. Of course, that might not stop a lawsuit in the event of a determined and disgruntled employee, but it certainly would offer a viable defense. Policy considerations are discussed further below, and it is recommended that both public and private sector employers adopt a policy on this subject.

B. State Workplace Laws

Additionally, several states have specific laws that limit or prohibit workplace monitoring. Though some of those laws may have been adopted prior to some of the more recent technological developments becoming commonplace, employers in those states must consider carefully whether and how to implement a monitoring program to keep it in compliance with the laws.

For example, Connecticut and Delaware require that an employer notify employees of electronic surveillance. Conn. Gen. Stat. § 31-48d (requires notice and a conspicuous posting that describes what electronic monitoring is being done); Del. Code Title 19, §705 (employer must provide notice of monitoring telephone transmissions, email, or internet usage). New York law prohibits an employer from "discriminating" against an employee for "legal recreational activities" that take place away from work (and off-duty) unless the activity creates a conflict of interest. N.Y. Lab. Law §201d. *See also* 820 Ill. Comp. Stat. 55/1-20 for similar requirement in Illinois. Several states have laws limiting where workplace surveillance can occur (for example, not in locker rooms or other places used by employees for "personal comfort").

All states have wiretap laws that may affect how it is done, but which do not generally prohibit an employer from capturing work-related information for business purposes. I will not address wiretap laws here, because they generally relate to wire and oral communications being intercepted at the point of communication, and most contain consent provisions.

C. Privacy Laws

Privacy considerations will vary depending on state law, and some considerations will overlap with state workplace laws like the ones discussed above. Some states have laws relating to surveillance and privacy in general that will also apply to the workplace, but which are not limited to workplaces. California's constitutional privacy provisions might limit workplace monitoring, potentially yielding a cause of action if the violation is "seriously offensive." Nebraska has a statutory right to privacy (Neb. Rev. Stat. 20-201 et. seq.), which is subject to an individual consent defense.

A breach of privacy claim appears unlikely to succeed where information is publicly available on the internet (such as where an employer does post-hire monitoring of employee's use of social media), where the employer has a clear policy on monitoring/tracking, or where the employer obtains explicit agreement to the monitoring (such as an employee agreement upon assignment of an iPad for work). In all such cases, there would be only a very low, or even no, reasonable expectation of privacy.

A few courts have addressed privacy claims in the employment context that involved monitoring or tracking. In *Elgin v. St. Louis Coca-Cola Bottling Co.*, 2005 WL 3050633 (E.D. Mo. 2005), the court rejected a claim that the employer violated the employee's privacy (actual claim: intrusion upon seclusion) through the use of a GPS tracking device on a company vehicle. The employee worked as vending machine technician and was assigned a company vehicle for those purposes, a vehicle he was allowed to use during non-work hours. In investigating a rash of cash shortages from vending machines, the company placed GPS trackers on all technicians' vehicles. After the investigation was complete, the employer told the employee what it had done, and cleared him of wrongdoing. The employee sued. In dismissing the claim, the court looked to Missouri law, which requires a showing of a secret matter, a right to keep that matter secret, and the invasion of that secret through unreasonable means. Here, the information revealed was limited to the whereabouts of the company vehicle. The court found that, especially because the vehicle was the employer's property, the company's use of the GPS tracker on its own vehicle "[did] not rise to the level of being highly offensive to a reasonable person." *Id.* at *4.

Could an employer track a personal vehicle? According to the New York Appeals Court reviewing an administrative proceeding, in *Cunningham v. New York State Dept. of Labor*, 89 A.D.3d 1347 (N.Y.A.D. 3 Dept. 2011), GPS tracking of an employee's personal vehicle was reasonable (one judge dissented). The New York State Department of Labor suspected an employee of submitting fraudulent time cards and referred the matter to the inspector general. To investigate, the OIG placed a GPS tracking device on the employee's personal vehicle and monitored it for several weeks. The monitoring revealed that the employee was submitting false expense sheets and other travel records. Following his termination, the employee sued. The court ruled that the use of the GPS data was permissible, because the use of the GPS tracking device, which was operational at all times including after work hours, was only monitored for one month by an investigator during work hours and used only to obtain "information relevant to [the employee's] location during work hours," was reasonable.

D. Work-Owned versus Personal Devices/Vehicles

Another consideration with legal implications is whether the employer is intending to or will monitor a privately-owned device (or track a personal vehicle). It feels intuitively correct that an employer can track employer-provided equipment or control the usage of that equipment. It does not, however, follow that similar monitoring or tracking of personal equipment would be acceptable. However, consider a workplace that allows an employee-owned mobile phone to receive workplace email accounts. Should the employer then be able to reach into that phone to wipe email or other data if the employee leaves their job? Does that email service being pushed to the mobile phone allow the employer to locate the phone through the communications between the phone and the server? As the *Cunningham* opinion shows, investigatory monitoring or tracking of personally-owned but work-used devices or vehicles may be reasonable – and more palatable than a general policy of monitoring personal devices or tracking personal vehicles.

E. Labor Unions

Finally, consideration must be given to whether employer programs to monitor computer or phone usage or social networking must be collectively bargained with unions representing units at the employer. Under the National Labor Relations Act, and under corresponding state labor relations laws, it is likely that a new or significant expansion of a program of workplace monitoring (such as GPS tracking) would be a mandatory subject of bargaining. This must be considered as policies are revised or adopted.

The NLRA also prohibits "surveillance" of employee communication that may constitute union organizing activity, which could occur on social media platforms. Employer monitoring of social media posts could, depending on the circumstances, run afoul of this restriction and lead to disputes before the National Labor Relations Board (including for non-union employers). The analysis often turns on how the employer first learns of the post or the extent to which an employer leads employees to fear that all posts will be monitored. Reviewing a post in the public domain is unlikely to be unlawful surveillance. Employers should, however, avoid accessing any password-protected site or creating any impression that employee posts on their personal sites will be actively monitored absent some connection to the workplace (ie., using an employer-owned computer to access the site). The NLRB has offered some guidance to employers on preparing social media policies that will pass legal muster.

III. Practical and Policy Considerations

A. Whether to Adopt a Policy and What to Include

Any institution determining whether to monitor employee internet or email usage generally should consider adopting a policy or revising existing policies to address the electronic environment (if it is not already addressed in those policies). For those institutions that are considering a one-off or investigatory exploration of someone's internet use or email traffic, a careful review of existing policies should happen pre-

search, especially if the institution is public or located in a state with a statute restricting employer surveillance. The Court in *United States v. Jones*, discussed above, found that warrantless GPS tracking of a vehicle for 28 days was a search. While this does not create a rule requiring employers, especially private sector employers, to inform employees of tracking programs or devices, it seems wiser to have explicit or implicit consent to the tracking. Public sector employers should also consider under what conditions tracking of a personal vehicle (or phone) would be considered or allowed.

On the whole, a policy that outlines the monitoring program, defines the reasonable expectation of privacy for employees, and categorizes the monitoring that an employee can expect offers the employer some protection in the event of legal dispute. The policy should make the program clear. Explain why the policy is being adopted – what are the expectations and goals. Explain whether the employer will monitor off-duty conduct and, if it will, under what conditions. Include a definition or statement of what equipment is covered and to what extent. Include a clear statement of what conduct is prohibited. One useful article is this July 2011 post by CAI to Workplace Insights – a North Carolina Employer's Handbook, outlining a series of do's and do not's for an electronic monitoring program. CAI, *E-Monitoring in the Workplace: Do's and Do Not's*, July 26, 201, ://blog.capital.org/e-monitoring-in-the-workplace-do%E2%80%99s-and-do-not%E2%80%99s/ (last accessed June 18, 2012).

Of course, a policy that nobody knows anything about, or which is not enforced, is in some ways worse than no policy at all, so it is also advisable to education your employees about the policy. The nature of the academic environment might suggest that employees should be in the crafting of such a policy.

B. A Brief Note About e-Discovery

The information about and from an employee monitoring program, as well as information gathered from system checks of Internet usage, is a record. As such, it should be considered as part of your institution's record retention program, and a decision should be made about how to handle it as electronically stored information in the discovery process. If your institution already has a record retention policy or practice with regard to email, it is possible that can be modified to apply also to this other data.

C. Other Considerations

Although workplace monitoring may increase productivity, there is a certain 'Big Brother' feel to the introduction of such programs that many managers may want to avoid. Workplace monitoring and employee tracking may also generate resentment, employee stress, and encourage employees to 'work to the standard.' A body of literature on such issues can be found in management and general business publications. Additionally, there are some legislative moves afoot at the federal level and in several states to limit an employer's ability to monitor employees, at work or on social media. A few states, such as New York, have already started in that direction. Others may follow.

"Blumenthal, Franken Call on Social Intelligence Corp to Clarify Privacy Practices"

On September 19 2011, Senators Richard Blumenthal (D-Connecticut) and Al Franken (D-Minnesota) sent a letter to Social Intelligence Corporation asking questions about how Social Intelligence's employment screening and monitoring services work as they relate to personal privacy. They wrote that they "are concerned that [Social Intelligence's] collection of online and social media information about job applicants and distribution of that information to potential employers may contain inaccurate information, invade consumers' right to privacy online, violate the terms of service agreements of the websites from which [Social Intelligence] culls data, and infringe upon intellectual property rights." So they asked a series of questions:

Accuracy of Information

1. How does your company determine the accuracy of the information it provides to employers?
2. Does your company have procedures in place for applicants to dispute information contained in the reports your company produces? If so, what are these procedures?
3. Is your company able to differentiate among applicants with common names? How?
4. Is your company able to determine whether information it finds on a website is parody, defamatory, or otherwise false? How?
5. Does your company accord less weight to certain sources of information that may be inaccurate, such as community-edited websites like Wikipedia?
6. Search engines like Google often provide archived versions of websites; these cached web pages may contain false information that was later updated. Search engines also provide "mirrors" of websites, like Wikipedia or blog articles; these mirrored pages may be archives of inaccurate information that has since been corrected. Is your company able to determine whether information it is providing is derived from an archived version of an inaccurate website? How?

Consumers' Right to Online Privacy

1. Does your company require the consent of a job applicant before conducting a background check on the applicant? If so, who requests the applicant's consent: your company, or the potential employer? Based on your experience with employers, does an applicant's refusal to consent to a background check by your company damage his or her eligibility for a job?
2. Does your company specify to employers and/or job applicants where it searches for information—e.g., Facebook, Google, Twitter?
3. Is the information that your company collects from social media websites like Facebook limited to information that can be seen by everyone, or does your company endeavor to access restricted information, for example by creating a Facebook profile with the same city and/or alma mater of an applicant, in an attempt to see information restricted by geographical or university network? Has your company ever endeavored to access a user's restricted information by joining the user's network of "friends" on sites like Facebook?
4. Companies like Google and Facebook have faced scrutiny in the past for making public portions of their users' information that the users had set as private, often without the consent of users. This has resulted in previously private information, such as pictures, being made publicly available against the wishes of the users. Users are then required to opt out of sharing information they had previously thought to be private. Does your company include such information in its reports?

5. If your company conducts multiple background checks on an applicant, to what extent does it reuse information it has collected in previous checks? If your company were to gain access to private information in a manner contemplated in the previous question, and found that it no longer had access to such information in a subsequent search, would it include the previously accessed information in subsequent reports?

Terms of Service and Intellectual Property Violations

1. The reports that your company prepares for employers contain screenshots of the sources of the information your company compiles. One publicly available report contains pictures of a user's Facebook profile, LinkedIn profile, blog posts for a previous employer, and personal websites. These websites are typically governed by terms of service agreements that prohibit the collection, dissemination, or sale of users' content without the consent of the user and/or the website. LinkedIn's user agreement, for example, states that one may not "rent, lease, loan, trade, sell/re-sell access to LinkedIn or any information therein, or the equivalent, in whole or in part." Your company's business model seems to necessitate violating these agreements. Does your company operate in compliance with the agreements found on sites whose content your company compiles and sells? If so, how?

2. More troubling than the apparent disregard of these websites' terms of service are what appear to be significant violations of users' intellectual property rights to control the use of the content that your company collects and sells. Your company includes pictures in its background reports; example reports have included a picture depicting the subject holding a gun to illustrate alleged "potentially violent behavior." These pictures, taken from sites like Flickr and Picasa, are often licensed by the owner for a narrow set of uses, such as noncommercial use only or a prohibition on derivative works. Does your company obtain permission from the owners of these pictures to use, sell, or modify them?

As printed in the Chicago Tribune on April 8, 2012

More than a friend request

Employer requests for Facebook access increase liability, employee resentment

JEFF NOWAK
Partner, Franczek Radelet

LUCIANO LOZANO/IKON IMAGES PHOTO

Picture yourself in the interview for the job of your dreams: You're sporting a fabulous new suit, you're nailing every question, and you've developed a rapport with your prospective boss.

As the interview draws to a close, he appears ready to invite you back for a second round. Then he offers one last question: "Would you provide me your Facebook password so we can access the content in your profile?" The intent is clear: This prospective employer wants to scour social media sites for any content that might effectively screen you out for employment.

Over the past few weeks, news outlets across the country as well as Facebook itself have reported that employers are increasingly seeking access to individuals' Facebook accounts to find out more about candidates. The outrage has been so intense and visceral, it's as if Bears fans just learned Mike Ditka had agreed to coach the Green Bay Packers.

At this early juncture, there are no good data indicating how many employers are engaging in this practice. I would venture to guess it's a mere handful. Nevertheless, late last month several U.S. senators called for Attorney General Eric Holder and the Equal Employment Opportunity Commission to investigate the legality of this practice.

Even local legislators have joined in: State Rep. La Shawn Ford, D-Chicago, recently introduced a bill in the Illinois General Assembly that would make it unlawful for an employer to ask a current or prospective employee to provide login information to their social media accounts or profiles. The bill would allow job seekers to sue if asked for such access.

To some extent, this practice should not surprise us. In the past few years it has become increasingly common for employers to review public social media profiles to learn more about job candidates. Some surveys put the number of employers doing so at more than 50 percent. So, as candidates have increasingly set their Facebook and other social media profiles to private, some employers are taking the next step, seeking direct access to them.

Facebook insists that employers should not ask for candidates' passwords because it's not the "right thing to do." As one who represents employers exclusively, I am one of the last to advocate for restrictions on employers' rights. However, beyond this question of "right or wrong," requesting passwords to social media accounts and profiles is not good business for a host of reasons:

■ It could expose the employer to discrimination claims. A fundamental best practice for employers when gathering information about prospective employees is to make sure that any inquiry is "job-related." When employers access a candidate's social media account, they lose control of the information presented and almost surely collect a lot of information that is not job-related and should never be considered in an employment decision.

Put another way, an employer would never require a candidate to submit a resume with a photo or ask about the candidate's race, age, religion or sexual orientation. Yet all of this information is potentially available through social media. Once an employer knows this, how does the employer unlearn it?

■ Employers also can be exposed to privacy claims. Social media effectively is the water cooler of the tech-savvy workplace; it's the busy intersection where employees gather to share deeply personal commentary and voice their complaints. Today's Facebook is like yesterday's snail mail; it's how a growing number of us communicate. Just as a prospective candidate wouldn't want an employer rummaging through his or her mail, it seems equally unseemly to allow the employer in the candidate's social media account or profile.

New legislative initiatives aside, employers accessing social media could be violating existing anti-eavesdropping and privacy laws, depending on the state.

■ Most employers are not prepared to handle this private information. Nearly all those requesting these passwords are not staffed to do so. And if the employer misses clear signs that the applicant may engage in conduct harmful to others, will the employer face liability for so-called negligent hiring?

After the employer is finished with the password, what does it do with it? Throw it out? Store it in the human resources department? In addition, the employer may have some responsibility for preventing the disclosure of this password to third parties.

■ Employer = Big Brother. Put aside the legal issues. When you ask for a prospective employee's password, it sends several messages that may seriously undermine your business goals. For one, it suggests that you lag in your knowledge and acceptance of social media. More important, it provides a glimpse of the Big Brother to come. It's as if you're telling a prospective employee: If I am asking for your passwords now, just wait until you start working for me. Also, applicants who readily submit passwords will assume that spying on fellow employees will be rewarded.

Requiring Facebook passwords is not good business. It's also not likely to reap meaningful benefits. It will take only seconds for an applicant to scrub their media posts after providing their passwords, thereby eliminating any benefit of asking. So why do it?

Jeff Nowak is a partner and co-chair of Franczek Radelet's labor and employment practice group, representing employers in all aspects of labor and employment law.

Outside Opinion is a forum for local business executives, economists, analysts and academics to discuss their take on the business topics of the day. Send submissions, suggestions, questions or comments to businessvoices@tribune.com.

City of Ginsburg, California
INTERNET REFERENCE POLICY

Policy number: 300.0

Policy name: Internet Reference Policy

Applicability: All new external job candidates

Date of approval: 15 April 2009

Date of next review: 15 April 2010

300.1 Statement of Policy

Internet soft referencing is an emerging human resources practice by which hiring managers use the Internet to research a job candidate's background and qualifications. This City of Ginsburg's Internet Reference Policy allows managers to use the Internet to research the background and qualifications of job candidates, while complying with court rulings and city policies that protect candidate's legal and constitutional rights. The purpose of this policy is to allow hiring managers to make more informed decisions and to hire the most-qualified candidates for vacant positions. The City of Ginsburg is committed to following policies and procedures in conjunction with all applicable laws when instituting this policy.

300.2 Policy Goals

Aligned with the City's goals of transparency and integrity, the City of Ginsburg has explicitly described goals of the Internet Reference Policy. These are to:

- Provide managerial flexibility to use all reliable information in hiring decisions;
- Protect city from unnecessary litigation by enforcing applicable federal, state and local laws;
- Protect candidate privacy rights;
- Protect candidate constitutional rights;
- Uphold equal employment opportunity policies and statutes;
- Ensure accuracy of information used in employment decisions;
- Protect merit hiring principles; and
- Provide transparency in hiring decisions.

300.3 Applicability & Scope

300.3.1 Intended for new hires for final consideration of a vacant job position. A hiring manager may only conduct an internet reference check of a candidate after the final round of interviews and only for the finalists for a position.

300.3.2 Not intended for use on active employees employed by the City of Ginsburg or those active employees being considered for promotion.

300.3.3 Not to be utilized for political appointees.

300.4 Limits to Use

300.4.1 Internet reference checks on job candidates are limited to information available to the general public, including information discoverable via any web-based search engine.

300.4.2 The content found within those searches may only be assessed and utilized based on policy. (Reference Section: Use of Reliable Information)

300.4.3 Hiring managers may not join or use any content from any members-only that is primarily social, familial or romantic in nature.

300.4.4 Hiring managers may search membership sites that are primarily professional in nature, including LinkedIn.com, HotJobs.com, Guru.com and professional association websites; however, hiring managers must respect privacy settings of a profile and may not compromise wishes of explicit privacy options.

300.4.5 Hiring managers may not use the Internet to violate the Constitutional rights protected by the Bill of Rights. These include, but are not limited to freedom of association, speech, religion as well as due process rights.

300.4.6 Job candidates have the most expansive right to freedom of speech on matters of public concern, newsworthy events and partisan topics, as delineated by the U.S. Supreme Court. Hiring managers may only discriminate against a job candidate based on speech regarding matters of public concern based on a "compelling need," such as a belief that the speech would substantially interfere with operation of the agency or impair the discipline of the work unit.

300.4.7 However, statements made in the course of a candidate's job performance – such as testimony at public hearings, public speeches and official reports -- are exempt from First Amendment protections and may be considered as hiring criteria.

300.4.8 Comments that are *not* related to matters of public concern, newsworthy events or partisan topics enjoy lesser protection from the law and this policy. A hiring manager may consider non-public concern speech if she or he has a reasonable expectation that the information relates to the candidate's likely job performance

300.4.9 Examination of content must be consistent with ALL Equal Employment Opportunity requirements, including but not limited to prohibitions on discrimination based on race, religion, sex, disability, national religion, or sexual orientation. Please refer back to EEO guidelines for all specification. If any information discovered reveals a candidate's protected class status, hiring managers cannot take into account (discriminate or endorse) at anytime during hiring or employment.

300.4.10 Internet shall be used for general background searches. If a criminal background check is necessary for employment, use the appropriate guidelines by submitting a request to the Department of Human Resource for processing through the California Attorney General's Live Scan process. Please see the Criminal Background Check Policy for a list of job classifications for which Live Scan searches are permitted.

300.4.11 Websites that explicitly state they are not to be used for employment purposes may not be used in internet references of candidates.

300.4.12 Any questions regarding legality, discrimination and questions around EEO should be referred immediately to the Human Resources legal department for clarification.

300.5 Use of Reliable Information

300.5.1 Hiring managers must assess the credibility of any information about a job candidate found on the Internet. While hiring managers are not required to prove the veracity of information, they must have a reasonable expectation that the information is gleaned from a credible source. Examples of credible information include – but are not limited to – newspaper reports, a candidate's published works or previous work products, and any content authored by the candidate that is available to the general public.

300.5.2 Hiring managers may not use unreliable information, such as Web logs by unaffiliated third parties, Wiki sites that contain malleable information, and other sites that are not authored or endorsed by a reliable institution or source.

300.5.3 In order to consider information found via Internet in hiring consideration, a hiring manager must be reasonably certain the information is actually referring to the job candidate, not some other person. A hiring manager may only search for information using the identifying information provided in the job application, including, but not limited to, names, e-mail addresses, social security numbers, Web site addresses and names of former employers.

300.5.4 Hiring managers shall attempt to verify any information prejudicial to a candidate before using it in a hiring decision. For example, the manager may ask a candidate or a reference to confirm that the candidate is indeed the subject or author of a Web posting.

300.6 Transparency Requirements

300.6.1 All information viewed in an internet reference check must be printed in hard copy or in electronic archival links and stored in HR department files two years, as per California law.

300.6.2 The Department of Human Resources must notify all job candidates of the City's intent to use an internet references and the candidate's Right of Appeal of any hiring decision based on the results of an internet reference check.

300.6.3 The results of an internet reference check will not be shared with job candidates.

300.6.4 This Internet Reference Policy will be made available for viewing on the city's Web site.

300.7 Appeal Process

300.7.1 A candidate who believes internet references unrightfully prohibited their employment with the City of Ginsburg may appeal the decision to the Director of Human Resources within 30 days of the hiring decision.

300.7.2 The Director of Human Resources shall notify candidates and hiring managers that it has received an appeal within 3 days.

300.7.3 The Director of Human Resources shall determine whether an internet reference played an unjust or illegal role in the hiring decision as described by the Internet Reference Policy or any other HR policy.

300.7.4 The appellant has the right to demand a public hearing of the appeal. Otherwise, the hearing will be held in closed session to protect the privacy of the job candidate.

300.7.5 The Civil Service Commission shall issue a final decision with 30 working days after receiving a referral from the Department of Human Resources.

300.7.6 All appeals material should be sent to the Civil Service Commission, 725 Phil Street, Ginsburg, CA 90956

Police Department

Authorization for Disclosure of Social Networking Information

I, _____, give permission to the Police Department Background Investigator to access my personal social networking accounts. If my accounts are set to "private" I will log into the account in the presence of the Background Investigator and allow him or her to review the contents of the account(s). I understand access to the account(s) must be granted immediately upon request.

I understand that the information contained within my personal social networking account(s) shall be considered as part of my background investigation. Any information showing illegal, immoral or unethical activities or behaviors that violate the standards of conduct established for the position for which I am applying may disqualify me from further consideration by the Police Department.

I understand that refusal to allow the Police Department Background Investigator access to my personal social networking account(s) will disqualify me from further consideration for employment with the Police Department.

I understand that if in the future it is determined that I failed to disclose all existing personal social networking accounts under my profile/control, may result in disqualification from the hiring process, discipline and up to and including termination.

Please provide complete and accurate answers on this form. All answers will be subject to verification. When you have completed and reviewed your answers, submit to your Background Investigator.

Legal name (First, Middle, Last, Suffix) _____

Nickname _____ Maiden Name: _____

Alias / Legal Name Changes (First, Middle, Last, Suffix) _____

Date of Birth _____ Gender: □ Male □ Female

Virtual Identities

Please provide e-mail addresses, screen names, nicknames, online names, handles and other identifiers you have used in the past three (3) years. Check if the address is shared with a spouse or another person. (**Note: Do Not Provide Password**(s)

E-mail address 1 _____ Shared □

E-mail address 2 _____ Shared □

E-mail address 3 _____ Shared □

E-mail address 4 _____ Shared □

If more space is required please attach additional sheets.

Online activities

Please list any websites you have hosted, run, or maintained. List the name and URL, if known.

Name	URL
Website 1 _____	http:// _____
Website 2 _____	http:// _____
Website 3 _____	http:// _____

If more space is required; additional space is provided below.

Social Networking (List each Social Networking site and each Account)

(examples: Facebook, Twitter, Blogs)

Account Name(s) _____

_____

_____

_____

If you have any additional information to add, please do so in the space provided below:

By signing this document, I am agreeing to provide the Police Department immediate access to my personal social networking accounts.

- ☐ I do not have a social networking account
- ☐ I authorize the Police Department access to my social networking account(s)
- ☐ I have social networking account(s) but I do not authorize the Police Department access to my social networking account(s) knowing this will disqualify me from further processing.

I certify that all of the information provided in this form is true and correct.

_____ _____

Applicant Signature Date

_____ _____

Witness Signature Date

Social Media Policy Content and Samples

Scores of higher education institutions have adopted social media "policies" or "guidelines" for several different reasons. The principal factors are (a) protection of institutional reputation, (b) increased regulatory and judicial scrutiny of employee/employer conduct on social media platforms, and (c) the desire to avoid or minimize personnel disputes. Discussion of common provisions in such guidelines and a list of sample policies that demonstrate the wide array of approaches different institutions have adopted are set forth below.

I. Common Policy Provisions

Below is a summary of many common substantive provisions of policies from higher education institutions regarding employee and employer use of social media platforms.

(1) Introductions

Because social media policies attempt to influence the very manner in which employees communicate, many institutions attempt to set a tone for such policies that will connect with their own campus community, bearing in mind each institution's unique culture. This is commonly done in introductory sections to the policy, such as the following examples:

> Social media are powerful communications tools that have a significant impact on organizational and professional reputations. Because they blur the lines between personal voices and institutional voices, [our institution] has been crafted by University Marketing and Communications to help clarify how best to enhance and protect personal and professional reputations when participating in social media.[1]

> This [policy] is to promote responsible engagement and dialogue between employees and students, prospective students and/or constituents. Whether or not faculty and staff choose to create or participate in a blog, wiki, online social network or discussion is his or her decision. However, emerging online collaboration platforms are fundamentally changing the way faculty and staff work and how they engage with each other, students, and the public.[2]

> We don't mean to turn you off from blogging by immediately inundating you with legalese, but we need to make clear our respective rights and responsibilities related to this service. So, the President and Fellows of [institution] offer these blogging services (the "Services") to you subject to the terms and conditions of use ("Terms") contained herein. By accessing, creating or contributing to any blogs hosted at [institution], and in consideration for the Services we provide to you, you agree to abide by these Terms. Please read them carefully before posting to or creating any blog.[3]

Common points of emphasis that emerge from review of these introductory statements include the importance of: (a) responsible use of an evolving medium; (b) institutional reputation; (c)

---

[1] Ball State University Social Media Policy, http://cms.bsu.edu/About/AdministrativeOffices/UMC/WhatWeDo/Web/WebPolicies/SocialMedia.aspx.
[2] Hutchinson Community College Web 2.0, Social Computing and Blogging, http://wwwcms.hutchcc.edu/www/handbook/policies.aspx?id=9146&.
[3] Weblogs at Harvard Law School, http://blogs.law.harvard.edu/terms-of-use.

personal responsibility for well-considered communication; and (d) writing that speaks to web-savvy audiences while also conveying the weight of legal considerations.

(2) Scope of Policy

Social media policies tend to apply to employee use of either (a) all social media platforms relating to performance of job duties, or (b) only those platforms developed and managed directly by the institution itself. It is important to state this scope clearly, repeatedly, and directly. An example of each of these two types of policy statements follows:

> All social media platforms: This policy establishes the criteria and procedure for creating a University presence or participation on social media sites on behalf of the University . . . [which] includes (1) media sites established by the University on University-owned domains, (2) accounts on external sites such as Facebook, LinkedIn, Twitter, YouTube, etc. on behalf of the University; and (3) personal accounts on external sites that are approved for use or participation by University employees as part of their job duties.[4]

> Only University-sponsored platforms: The guidelines in this document are here to help inform your conduct while managing or interacting with a social media profile officially affiliated with [the University.] Note: Personal social media pages that include references to the University or links to groups affiliated with the University are NOT considered "officially affiliated" for the purposes of these guidelines.[5]

Regardless of which approach is selected, nearly all policies explain that employee use of any social media platform for personal reasons while at work should be minimal: "personal use of University electronic resources to access social networking sites is to be limited to incidental use," which "must not interfere with an individual's performance of his/her assigned job responsibilities or someone else's job performance or compromise the functionality of the department or campus network."[6]

(3) Employee Use – General Advice

Nearly every policy includes a general statement of "common sense" tips for employee use of social media platform. For example:

> When using University electronic resources to access on-line social networks, University community members (academic staff and employees, students and others) are expected to act

[4] University of Kentucky, Office of Public Relations and Marketing, Social Media Approval Policy, www.uky.edu/Graphics/SocialMediaPolicy.doc.

[5] Southeast Missouri State University, Social Media Guidelines, http://www.semo.edu/president/images/WDS_SocialMediaGuidelines_2010-04-27.pdf.

[6] Southeast Missouri State, Social Media Guidelines http://www.semo.edu/president/images/WDS_SocialMediaGuidelines_2010-04-27.pdf. *See also,* Ohio State University Medical Center: Social Media Participation Guidelines, http://www.scribd.com/doc/27664236/Ohio-State-University-Medical-Center-Social-Media-Participation-Guidelines, (only during non-work time for personal use); DePaul University Social Media Guidelines, http://brandresources.depaul.edu/vendor_guidelines/g_recommendation.aspx ("you should maintain your personal sites on your own time using non-[university] computers").

> with honesty, integrity, and respect for the rights, privileges, privacy, sensibilities, and property of others.[7]
>
> If you wouldn't put it on a flier, carve it into cement in the quad or want it published on the front of the Wall Street Journal, don't broadcast it via social media channels.[8]

Many policies also include a list of specific concepts and warnings, often presented as bullet points, that emphasize the importance of: (a) the permanent nature of online postings; (b) transparency regarding identity; (c) accuracy of facts; (d) respectful tone and language; (e) exercising discretion; (f) protecting personal identity; and (g) including disclaimer of institutional affiliation whenever posting in personal role.[9]

(4) Monitoring or Removing Content and "Privacy"

Every policy should address the extent to which the institution can or will monitor social media platforms as well as the potential for the institution to use employees' postings found during such monitoring. For platforms sponsored by the institution, most policies include a reservation of complete discretion to monitor and remove offensive or inappropriate postings.[10] For platforms hosted by others, references to institutional monitoring of use on the institution's computers tends to be less direct.[11] However, even in such situations, an institution may reserve the right to investigate, in response to complaints, profiles on social networking platforms and "use the information in informal or formal proceedings."[12]

Perhaps because social media policies address institutional monitoring, they tend not to contain specific provisions regarding employees' expectation of privacy. Instead, that issue is commonly addressed in "computer use" or "computer ethics" policy provisions that establish employee privacy expectations for all electronic communications that occur on institutional computer equipment, including social media platforms. For example:

> Users should be aware that their use of Electronic Resources is not completely private . . . . The university may also monitor, access or modify the contents of Electronic Resources of individual users without notice, in circumstances where a senior official determines that it is necessary to do so. These circumstances are described in more detail in the *Guidelines.*
>
> * * *
>
> The university may monitor the activity and accounts of individual users of university computing resources, without notice, when (a) the user has voluntarily made them accessible to the public,

---

[7] Guide for UCSB Employees, Departments, and Registered Organizations http://www.policy.ucsb.edu/policies/advisory-docs/social-networking-guide.pdf.

[8] Seattle University Social Media Guidelines, http://www.seattleu.edu/marcom/Inner.aspx?id=51927.

[9] DePaul University Social Media Guidelines, http://brandresources.depaul.edu/vendor_guidelines/g_recommendation.aspx; University of Michigan Guidelines for the Use of Social Media, http://www.voices.umich.edu/announcements/socialmedia.html; Seattle University Social Media Guidelines, http://www.seattleu.edu/marcom/Inner.aspx?id=51927.

[10] Washington University in St. Louis Social Media Policy, http://wustl.edu/policies/socialmedia.html, (university "shall have the right to remove, at its sole discretion, any content that it considers to violate this policy").

[11] See Guide for UCSB Employees, Departments, and Registered Organizations http://www.policy.ucsb.edu/policies/advisory-docs/social-networking-guide.pdf, (institution "doesn't routinely monitor social networking sites" but "may perform activities necessary to ensure the integrity, functionality and security of the University's electronic resources").

[12] *Id.*

> as by posting to a blog or a web page; (b) it reasonably appears necessary to do so to protect the integrity, security, or functionality of university or other computing resources or to protect the university from liability; (c) there is reasonable cause to believe that the user has violated, or is violating, the Electronic Communications policy or guidelines; (d) an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or (e) it is otherwise required or permitted by law.[13]

Because the extent of an employee's privacy at work, under the law of most states, hinges on the expectations established by their employer, it is prudent to include in social media policies at least a cross-reference to the institution's general policy statement regarding the privacy of electronic communications. Adding some warning about employer access to such information can also help educate employees before they post anything and avoid disagreements.

(5) University-Sponsored Platforms

The substantive provisions of statements governing employee use of institution-sponsored social media platforms contain several common elements. Many take great care to:

- Require institutional approval to create such a platform;
- Define a process for obtaining approval; and
- Identify particular individuals or offices that control that process (e.g. provosts, executive vice-presidents, presidential councils, department heads, and communication or marketing managers.[14]

Establishing an approval process is important to maintain consistency for the institutional "image" presented to the public by such platforms and to ensure awareness of the mere existence of all such platforms by a particular person or office. Consistent with these goals, such policy statements also explain requirements or guidelines for the appearance of such platforms (use of logo, consistent color schemes, etc.), and even the selection of the name of such platforms.[15] As mentioned above, university-sponsored platforms are commonly subject to heightened monitoring expectations, which set forth the institution's right to monitor and remove content explicitly, such as:

> You acknowledge that [university] does not pre-screen or regularly review posted content, but that it shall have the right to remove in its sole discretion any content that it considers to violate

[13] The Catholic University of America, Employee Electronic Communications and Resources Policy, http://policies.cua.edu/infotech/eec.cfm and Employee Electronic Communications Guidelines, http://computing.cua.edu/procedures/electroniccommunications.cfm.

[14] *See* University of Kentucky, Office of Public Relations and Marketing, Social Media Approval Policy, www.uky.edu/Graphics/SocialMediaPolicy.doc; Hutchinson Community College Web 2.0, Social Computing and Blogging, http://wwwcms.hutchcc.edu/www/handbook/policies.aspx?id=9146&; Seattle University Social Media Guidelines, http://www.seattleu.edu/marcom/Inner.aspx?id=51927; Ohio State University Medical Center: Social Media Participation Guidelines, http://www.scribd.com/doc/27664236/Ohio-State-University-Medical-Center-Social-Media-Participation-Guidelines.

[15] *See* Seattle Univ. Social Media Guidelines, http://www.seattleu.edu/marcom/Inner.aspx?id=519 (establishing guidelines for naming platforms and stating "[n]aming your social media channel is very important. Please note, that you will not be recognized as an official communication channel of the university unless you adhere to these naming guidelines").

> these Terms or the terms of any other campus user agreements that may govern your use of the campus networks.[16]

Policies for such platforms also often include references to the importance of regularly updating information and a requirement to identify a particular person responsible for that role.[17]

(6) Criticism of the Employer

Although often part of a policy relating to University-sponsored platforms, most institutions tread carefully when restricting employee comments that reflect negatively on the employer-institution. This has become all the more important in light of the NLRB position and litigation regarding employee criticism on Facebook and protections for such criticism as union-organizing activity. For example, one policy states:

> If an employee . . . is using a University-affiliated social media presence to criticize or discredit the University, the employee will be asked to edit the offending material. In extreme cases the employee may be subject to enforcement of the IT Acceptable Use Policy.[18]

Some institutions even encourage public debate regarding controversial issues pertaining to issues on campus, including:

> Acceptable content may be positive or negative in context to the conversation, regardless of whether it is favorable or unfavorable to [the institution].[19]

Conversely, other campuses have adopted policies that more explicitly direct employees not to criticize their employer publicly, even on their own personal platforms, as follows:

> Your personal social media account is not an appropriate place to distribute university News. If you have University information and news that you would like to announce to the public or media, please contact [university marketing and communications].[20]

> Avoid discussing or speculating on internal policies or operations . . .A healthy dialogue with constructive criticism can be useful but refrain from engaging in dialogue that could disparage colleagues, competitors, or critics. . . . Please refrain from reporting, speculating, discussing or giving any opinions on university topics or personalities that could be considered sensitive, confidential or disparaging.[21]

It bears repeating that, in light of the NLRB's position with respect to employees' right to post negative comments on their personal social media accounts, any statements restricting employee criticism of the institution raises potential for legal disputes and should be carefully reviewed.

---

[16] Weblogs at Harvard Law School, http://blogs.law.harvard.edu/terms-of-use/.
[17] *See* University of Kentucky, Office of Public Relations and Marketing, Social Media Approval Policy, www.uky.edu/Graphics/SocialMediaPolicy.doc ("at least one faculty or staff person shall be designated to monitor the medium, identify problems that emerge, and take action when necessary").
[18] Southeast Missouri State Social Media Guidelines, http://www.semo.edu/president/images/WDS_SocialMediaGuidelines_2010-04-27.pdf.
[19] Washington University in St. Louis Social Media Policy, http://wustl.edu/policies/socialmedia.html.
[20] Seattle University Social Media Guidelines, http://www.seattleu.edu/marcom/Inner.aspx?id=51927.
[21] Seattle University Social Media Guidelines, http://www.seattleu.edu/marcom/Inner.aspx?id=51927.

(7) Confidential Information

One universal directive in social media policies is the instruction that employees not post confidential data or other protected institutional information on social media platforms. Categories of such data include: (1) personnel information regarding subordinates or colleagues (such as disciplinary information); (2) information protected by FERPA or HIPPA; (3) proprietary information of others, such as information protected by copyright/trademark; or (4) the institution's own proprietary information, such as logos.[22]

(8) Hiring

Few policies address employer use of social media platforms to gather information about candidates for positions in the hiring process. Those that do seek to clearly define (1) the extent to which hiring decisions can be based upon information learned from any social media sites and (2) the risks inherent in doing so. For example:

> Use of social media sites for recruiting cannot be the only or primary source for recruiting as this may adversely impact the diversity of your applicant pool. These sites can be used to post information about an opportunity at the University; they should not be used to look for or screen applicants. Such action could violate principles of Affirmative Action if certain identifying information is gained.[23]

In addition, these provisions often establish mechanisms that must be used to (1) notify applicants of the intent to do so, (2) advise any applicant if information that has been found and will be used in evaluating their application, and (3) permit the applicant an opportunity to explain the information.[24]

(9) Disciplinary Provisions

Many social media guidelines include provisions regarding potential discipline for failures to adhere to the guidelines, including the following examples:

> Public Relations and Marketing is charged with the responsibility to monitor the University's social media initiatives, counsel those who represent the University online on adherence to these policies, and take action to restrict or remove an employee's ability to "publish" should efforts to correct the situation fail. If disciplinary action seems necessary, Human Resources shall be consulted and will determine an appropriate course of action for staff employees. For faculty, the appropriate dean or the Associate Provost shall be contacted and will determine an appropriate course of action.[25]

---

[22] Southeast Missouri State University, Social Media Guidelines, http://www.semo.edu/president/images/WDS_SocialMediaGuidelines_2010-04-27.pdf; University of Minnesota, Social Networking, http://www1.umn.edu/brand/requirements-and-guidelines/social-networking/.

[23] Social Media Use on the Internet, A Guide for University of Iowa Employees, www.uiowa.edu/hr/administration/social_media.html.

[24] Social Media Use on the Internet, A Guide for University of Iowa Employees, www.uiowa.edu/hr/administration/social_media.html; *see also* University of California, Santa Barbara, Using Internet Information in the Recruiting Process, http://hr.ucsb.edu/employment/internet_info.php (separate from social media policy).

[25] University of Kentucky, Office of Public Relations and Marketing, Social Media Approval Policy, www.uky.edu/Graphics/SocialMediaPolicy.doc

> Violations of policies on computing and electronic communications should be reported to the Director of Information Services or the Vice President for Human Resources. Violations will generally be treated in the same manner as violations of other University policies. If violations appear to constitute a criminal offense, as defined by local, state, or federal statutes, the appropriate authorities will be notified.[26]
>
> In the event that the university believes an employee has violated any part of this policy the university may suspend or terminate the employee's access to electronic communications systems and equipment. In addition, violation of this policy may subject employees to disciplinary action, up to and including discharge from employment.[27]
>
> There is one area of official policy regarding social networking sites, and that is to exercise freedom of speech with responsibility. If activity on a social networking site is reported as violating campus policy as outlined in the [college] student handbook, it will be investigated and handled according to the college disciplinary process.[28]

(10) Cross-Referencing Existing Policies

Because social media policies often restate existing rules regarding employee conduct in Web 2.0 context, many guidelines explicitly cross-reference other policies. A particularly thorough example contains a separate "Existing Policies" subsection, which includes references and links to the institution's policies regarding: (1) acceptable computer use, (2) copyright, (3) IT security, (4) personnel records and privacy, (5) privacy generally, (6) web site requirements and guidelines, (7) FERPA, (8) faculty and staff handbook, (9) student handbook, (10) procurement rules and contract manual.[29]

(11) Posting Photographs or Video

Photographs or videos posted on social media platforms present increased risks of liability, disputes, and problems, which can be addressed as follows:

> (1) Photos of children should not be posted without expressed consent from the parents. Even then such photos should be avoided;
> (2) Care should be taken not to post photos of individuals who would object. This may involve obtaining the appropriate permissions;
> (3) Photos posted on social networking sites must be appropriate. As a guideline, they should be photos that could be posted on the college's official Web site. Examples of photos that should be avoided include but are not limited to: photos involving alcohol, nudity, medical and hospital patients, and graphic scenes; and
> (4) Appropriate photo credits should be given. Social networking sites still represent [the institution], and any agreed-to-credits must be maintained.[30]

---

[26] Marylhurst University, Computing and Electronic Resources Acceptable Use Policy, http://docs.marylhurst.edu/mu/pdflibrary/IS-ComputingPolicy.pdf
[27] The Catholic University of America, Employee Electronic Communications and Resources Policy, http://policies.cua.edu/infotech/eec.cfm.
[28] Morehouse College Guidelines for Social Networking, http://www.morehouse.edu/news/policy.html.
[29] Colorado State University Policy, http://policies.colostate.edu/PolicyIndex.aspx.
[30] Morehouse Guidelines for Social Networking, http://www.morehouse.edu/news/policy.html.

II. Where to Find Sample Social Media Policies & Guidelines

Below is a list of and links to social media policies and guidelines at higher education institutions that are particularly helpful samples of the topics addressed above. In addition, a longer list of such policies in and outside of academia is assembled at the following online database: ://socialmediagovernance.com/policies.php.

Tufts University
://webcomm.tufts.edu/socialmedia

University of Kansas
://smbp.classcaster.net/files/2010/07/KUFacebookGuidelines.doc

University of Michigan
://voices.umich.edu/docs/Social-Media-Guidelines.pdf

Colorado State University
://socialmedia.colostate.edu/page/Social-Media-Policy.aspx

Seattle University
://www.seattleu.edu/marcom/Inner.aspx?id=53083

University of Kentucky
://www.uky.edu/Graphics/SocialMedia.doc

Washington University
://www.wustl.edu/policies/socialmedia.html

Ball State University
://cms.bsu.edu/About/AdministrativeOffices/UMC/WhatWeDo/Web/WebPolicies/SocialMedia/Guidance.aspx

Florida International University
://webcomm.fiu.edu/2009/05/social-media-guidelines/

University of Oregon
://des.uoregon.edu/stylemanual.pdf, also ://webcom.uoregon.edu/node/38

DePaul University
://brandresources.depaul.edu/vendor_guidelines/g_socialmedia.aspx

Vanderbilt University
://web.vanderbilt.edu/resources/social-media-handbook/

Using Internet Information in the Recruiting Process: Understanding the Risks

Many of you have asked for guidance on whether or not to use the Internet, including social networking sites such as MySpace or Facebook, as part of the job applicant screening process. While we understand the appeal of having access to so much additional information about prospective applicants, there are risks to using Internet information to screen job applicants. It is critical to understand the risks when you consider whether or not to use Internet information as part of the recruiting process. You are strongly urged to confer with Human Resources before using Internet information in any way as the basis for selecting or eliminating a candidate.

The risks associated with the use of Internet Information in the recruiting process include:

Discrimination Risks

California law prohibits the use of certain types of "off-duty" behavior as the basis for an employment decision. In addition, a simple online photo or "profile" may contain a wealth of information about a person's race, religion, national origin, sexual orientation, disability, age (40+) etc., and these factors ***cannot*** be taken into account in making hiring or other employment decisions under both state and federal law. Use of this type of Internet information to pre-screen job applicants could lead to a hiring discrimination claim -- that is to say, a claim that you used Internet information to screen out applicants on the basis of a protected category such as those listed above, or on the basis of legal off-duty behavior.

Information Reliability Risks

Not all the information you find on the Internet is reliable. The "name" you find on your Internet search may not actually be your applicant (statistics show that most of us have "computer twins," that is to say people with our names and even a similar date of birth). There are even anecdotes of false postings created under another person's name – a form of "cyber identity theft." Finally, an applicant may simply have exaggerated or invented certain facts or stories for fun, or for a variety of other reasons.

Privacy Risks

While it might seem like anything on the Internet is "fair game" to a prospective employer, a job applicant might actually have a reasonable right to privacy in certain online information, especially where access to the site has been restricted (for example, when only "friends" can view profile information). More importantly, trying to obtain information on job applicants through the use of multiple identities or "pretexting" (meaning through the creation of an "alter ego" or false identity) may violate not only the rules of the social networking site, but the user's privacy rights as well.

Because of these risks, if you choose to use Internet information as part of the recruiting process, please follow these guidelines to ensure that the information you find is used in a fair, non-discriminatory way that respects our job applicants' privacy.

- Do not search the Internet to prescreen applicants.
- Interview a job applicant in person before conducting an Internet search about the individual.
- Only after all the personal interviews are complete should an Internet search be used, if at all.
- If a search is done, it should be done for all final candidates.
- Information that you find must not be used to discriminate unlawfully against job applicants.
- Information must be obtained ethically and in a way that does not violate privacy permissions.

If you have any questions, please contact Human Resources - Employment