I. Introduction

The statistics on social media use are staggering. There are over 1.7 billion usernames registered to the top four social networking sites (SNS) (that’s Facebook, Twitter, Google+, and LinkedIn). Facebook alone receives over 100 billion hits per day. In Quarter 1 of 2012, Apple sold more iPhones than there were babies born in the world. In late 2011, a study indicated that the average cell phone user between the ages of 18 and 24 sends or receives 110 text messages per day. It is safe to say that wireless technology and online social networking sites have changed the way people connect and communicate.

These technologies have also changed the way employers make decisions. With a few quick keystrokes, employers can access a wealth of information, oftentimes very personal, about applicants and current employees. But these avenues for information create a myriad of questions. When can an employer use information learned from social networking sites in employment decisions? Can an employer search the cell phone of an employee if that phone is paid for by the employer? To what extent can employers regulate employees’ use of social networking sites?

This paper will analyze these and other questions employers often face. It will also look at current and emerging trends in employers’ use of social media and technology, and the resulting potential for liability. Finally, this paper will suggest practices that employers can use to mitigate their exposure to liability.

The author expresses his appreciation to Scott Selix, Summer Associate at the Ahlers Law Firm, for his assistance in the preparation of this paper.

---


II. Using Social Media In Hiring and Retention Decisions

a. “Googling” or “Facebooking” Candidates or Employees
With almost 2 billion usernames registered at various social networking sites (SNS), it seems that everyone has a social media profile. Many employers now use SNS as a part of the vetting process for potential hires. Employers can quickly learn a great deal by simply “Googling” or “Facebooking” an applicant. Generally, employers are allowed to use the information they glean from these sites in hiring decisions.\(^5\)

However, a quick glance at the social networking profile of a job applicant can reveal protected information about that applicant. For example, most Facebook profiles contain a picture of the user. This may give the employer insight into the applicant’s race, gender, or approximate age. Many profiles list a date of birth, hometown, religious affiliation, marital status, or sexual orientation. Further, sites like Facebook and Twitter allow users to post messages, potentially providing the employer access to other protected information. Even if the employer doesn’t use this protected information in its hiring decisions, the mere knowledge of an applicant’s status within a protected class could expose the employer to claims of discriminatory hiring practices.

A recent case illustrates the potential liability that employers face.\(^6\) In Gaskell v. University of Kentucky, Civil Action No. 09-244-KSF (E.D. Ky. 2010), a University of Kentucky employment decision-maker found the personal website of Dr. Gaskell, an applicant for the open position of Director of the University observatory, after “Googling” the name of the applicant. Upon learning Dr. Gaskell favored the religious view of creationism over evolution, the University decided to hire a significantly less qualified candidate. The University believed that the religious views of Dr. Gaskell could be detrimental to its science department. Dr. Gaskell subsequently brought suit against the University, alleging religious discrimination. In the end, the claim resulted in an undisclosed out of court settlement.

However, even in the aftermath of cases like Gaskell, it is equally clear that employers should not altogether ignore information gathered from the internet and SNS. Suppose an employer decides to “Google” an applicant and finds a video of the applicant driving excessively fast through a residential neighborhood. If the employer disregards that information and hires the applicant, who later hits and injures a pedestrian while driving in excess of the speed limit in a vehicle owned by the employer, the employer may be subject to a number of claims, including negligent hiring. Clearly, employers face a dilemma between the desire to hire and retain the best possible candidates and the potential liability from going too far in its investigation of applicants.

Another problem can arise when investigating applicants through SNS. Suppose you receive an employment application from a person named Matt Smith, and Mr. Smith lists the University of Iowa as his alma mater. A quick search on Facebook for Matt Johnson at the University of Iowa returns ten matching Facebook user profiles. At least nine of these are not the profile of the applicant named Matt Smith. Matt Smith, the applicant, may not even have a

---
\(^6\) Michelle Sherman, Social Media Research + Employment Decisions: May Be a Recipe for Litigation, 16 No. 3 Cyberspace Law. 1 (2011).
Facebook profile. Further, maybe friends of Matt Smith decided to make a parody page of him, or worse, maybe classmates of Matt competing with him for a job made a profile to sabotage Matt’s job prospects. Employers must be very careful to ensure that information revealed through investigations of SNS is accurate.

So what should employers do? First, employers need to decide whether they will conduct any social media investigation of applicants for employment. Second, if employers decide to do so, they must be uniform and consistent in their investigation protocol: all searches should include the same SNS, should examine the same data at each site, should apply to all applicants for employment or to all applicants for designated classes of employees whose position expose the employer to greater risk of liability, should include a process for preserving evidence of the investigation, and should provide a process for review with the applicant if the information has any adverse consequence. Third, employers need to separate the person making the hiring decision from the individual responsible for investigating the applicant. The person who does the investigation of the applicant’s social networking profile should transmit only non-protected information to the person making the hiring decision. For example, suppose an employer investigates the social media profile of an applicant for a position as a delivery driver. If the employer learns that the applicant is a forty-year-old white female that often uses marijuana while driving, the employer should ensure that the person responsible for making the hiring decision is only apprised of the candidate’s drug use while driving. In this way, employers can effectively vet applicants through social media, yet ensure that protected information is not used in the hiring decision. Companies like Social Intelligence Corp. offer screening and investigation services to employers, providing an additional layer of protection since the investigation is done by a third party.

In addition, employers need to be sure that the information they receive is accurate. If employers are unsure of whether they are looking at the right social media profile or whether the information may be taken out of context, employers should refrain from using that information in the hiring decision. As always, employers should be sure to provide a detailed record of the processes and information used when making a hiring decision, particularly if SNS are involved. Employers should put as much distance as possible between the protected information and the hiring decision. An employer that can show it did not have protected information when making an employment decision will be able to effectively defend a discrimination lawsuit.

I recommend that employers consider inclusion of the following statements in their employment application process whether or not they choose to actively use social media sites for their hiring decisions:

**Notice: TO APPLICANTS AND EMPLOYEES**

To the fullest extent permitted by state and federal law, the Employer will consider all information concerning an applicant or an employee in making hiring, firing and other employment-related decisions. The term “all information” includes information of any

---

kind (verbal, written, photographic, videographic, etc.) that is accessible in any medium (print, electronic, etc.) from any source. The Employer will consider public information and other information to which it has lawful access. This may include information that is contained in social networking sites, blogs, and other electronic sites, such as YouTube. If there is information that pertains to you that you believe requires explanation, interpretation, or clarification when it is considered by the Employer, it is your obligation to communicate this information to the Employer. Information that is relevant to the Employer’s decisions will be considered regardless of the date on which the Employer obtains the information and regardless of the date on which the information was first published, created, or made accessible to the Employer. **Individuals who provide false, inaccurate, or incomplete information in the application form, in an interview, or any other part of the hiring process or who fail to disclose information requested in the application form, in an interview, or any other part of the hiring process will not be eligible for employment, or, if they are hired, they will be subject to termination.**

To more fully protect the employer and insure that the applicant or employee is aware of the significance of this notice, the employer should require applicants or employees to sign the following acknowledgement:

**APPLICANTS:** I have read and I understand the notice provided to me by the Employer regarding information that the Employer may consider in making hiring, firing, and employment-related decisions. I acknowledge that I have been given the opportunity to provide information to the Employer that I wish the Employer to consider in making its decisions.

**EMPLOYEE:** I have read and I understand the notice provided to me by the Employer regarding information that the Employer may consider in making employment-related decisions. I acknowledge that I have been given the opportunity to provide information to the Employer that I wish the Employer to consider in making its decisions.

Finally, applicants for employment should be required to sign a verification statement:

I hereby certify that the statements made by me in this application and all related information which I have provided are true, accurate and complete to the best of my knowledge. I understand that if I provide any false, inaccurate, or incomplete information, I will not be eligible for employment, or, if I am hired, I may be terminated regardless of the date on which the Employer discovers information concerning a violation of this certification.

**b. Requiring Applicants or Employees to Divulge SNS Usernames and Passwords**

With the proliferation of social media, many aggressive employers are now requiring job applicants and current employees to disclose their social media usernames and passwords to the
employer. Applicants and employees who refuse are then either removed from consideration or terminated. While shocking to some, the practice itself is not illegal for private employers in most states (not yet anyways). If implemented by public employers, the practice is may be a violation of the Fourth Amendment.

Maryland recently became the first state to pass legislation forbidding all employers from requiring that potential or current employees divulge their private usernames and passwords as a condition of employment. Several states have introduced similar legislation, and a federal bill has been proposed that would prohibit the practice.

Employers face greater potential liability for discrimination claims when they require applicants and employees to divulge their personal SNS usernames and passwords. While applicants and employees often limit the amount of “public” information (that is, information accessible to all users) on their social media profiles, employers with the candidate or employee’s username and password have access to a wider range of private information. Additionally, an employer who requires disclosure of social media usernames and passwords puts applicants and employees on notice that they may be accessing protected information. Even if the protected information is not used in the employment decision, an employer who requires disclosure of personal usernames and passwords will face an uphill battle in trying to assert that it did not use or have knowledge of protected information. After all, why would an employer ask for a username and password if it were not going to use it?

It is dangerous for employers to require disclosure of SNS usernames and passwords of applicants or employees. Recent decisions and indications from legislatures point in favor of employers implementing policies that prohibit this practice by its supervisors. Public employers should implement a policy strictly forbidding supervisors from requesting SNS usernames and passwords from its employees. This kind of policy will limit employers’ exposure to liability and likely will foster more satisfied employees. As previously stated, employers should always attempt to distance themselves as much as possible from protected information.

III. Using Social Media When Terminating Employees

While cases involving discrimination due to social media in hiring decisions are rare, discrimination suits for wrongful discharge are increasingly common. It is easy to see why there is such a disparity in the numbers of each type of suit. Job applicants may never know the reason they did not receive an interview. They may not even know if the employer looked at the application. On the other hand, employers who are terminated are much more informed of the

9 Id.
10 Id.
11 Youndy C. Cook et al., The National Association of College and University Attorneys, Employers Use of Web 2.0: Take This Job and Twitter It (March 2011).
circumstances surrounding their termination. Employers should be extremely cautious before taking adverse employment action against its employees based upon the employee’s internet or social media conduct.

Social media is so widespread that almost all employers can expect that at least some of their employees are social media users. When an employee uses social media for browsing or socializing during working hours on a work device in violation of a company policy, there is little doubt the employer is safe if it terminates the employee. But what about when an employee posts disparaging remarks about the company during nonworking hours? Or when an employee sends an email complaining about a manager to coworkers? Several balancing rights and interests make the problem much less simple.

a. NLRA Section 7

Section 7 of the National Labor Relations Act protects employees when they engage in concerted activity. In particular, employers cannot discipline employees for discussing wages, hours, working conditions, or other terms of employment. Section 7 undoubtedly extends to discussions that occur over the internet. Increasingly, employers are facing lawsuits after terminating employees for posting negative comments about their employers on a social media website.

For example, in American Medical Response of Connecticut, Inc., Case No. 34-CA-12576 (Region 34, NLRB), an employee of American Medical Response posted disparaging comments about her supervisor and working conditions. Several coworkers responded to an initial post, which prompted the employee to post additional negative comments. When American Medical Response terminated the employee, she brought a claim against the company for a violation of her Section 7 rights. In finding for the employee, the National Labor Relations Board (NLRB) found that the posts were protected concerted activity. The NLRB also found that the social media policy of American Medical Response was overly broad, thereby restricting Section 7 rights.

One thing to note regarding Section 7 is that an employer need not take adverse employment action against an employee in order for there be a Section 7 violation. In the American Medical Response case, the NLRB found that the social media policy itself tended to chill protected concerted activity, and was therefore in violation of Section 7 of the NLRA.

The NLRA requires employers to analyze the speech of its employees. If the speech includes a discussion of wages, hours, working conditions, or other conditions of employment and might solicit responses from coworkers, the speech is likely protected concerted activity. Employers should always consult with legal counsel before they discipline or discharge employees for statements made by employees concerning these protected topics.

b. First Amendment Right to Free Speech

Employees disciplined for social media activity also often claim that the disciplinary action violates their First Amendment Right to Free Speech. In general, employees have a hard time prevailing on these claims, and public employees face an even greater uphill climb.

The Supreme Court of the United States has repeatedly held that public employees enjoy lesser First Amendment protection than the general public. Public employers may actually impose greater restraints on employees’ speech that would be unconstitutional if imposed on the general public. If public employees are acting in their official capacity, First Amendment protection of free speech extends only to speech on matters of public concern. The rationale for this exemption is that public employees may be uniquely qualified to comment on these matters. First Amendment protection does not extend to public employees who speak on a purely private employment matters, such as the dissatisfaction of an employee with his or her working conditions (though Section 7 may apply).

The standard is different, however, when public employees speak on their own time on topics unrelated to their employment. In order to regulate this speech, public employers must show some “governmental justification far stronger than mere speculation.” For instance, in Spanierman v. Hughes, 576 F.Supp2d 292 (D. Conn. 2008), a school district terminated a teacher for his conduct on MySpace. The teacher used his MySpace profile to connect with students and engage in public conversations, some involving the sex life of his students. After finding the teacher was not acting pursuant to his official duties, the Court found that the conduct of the teacher was sufficiently disruptive to school activities to justify regulation of his speech (and, therefore, his termination).

An interesting case is on appeal in the 4th Circuit. In Bland v. Roberts, 2012 WL 1428198, ____ F.Supp.2d ____ (E.D. Va. 2012), the court was asked to interpret what constitutes “speech” as it pertains to social media. A deputy sheriff to the sheriff running for reelection “Like” a Facebook page relating to the campaign of a challenger to the sheriff’s position. After the current sheriff was reelected, he immediately fired the deputy sheriff. The deputy sheriff then brought suit against the sheriff, claiming a violation of his First Amendment Right to Free Speech. The Deputy Sheriff argued that “Liking” a political Facebook page is akin to placing a political sign in your yard advocating a particular political candidate, speech that is undoubtedly protected by the First Amendment. The court ruled in favor of the defendant sheriff, finding that “Liking” a Facebook page is insufficient to amount to speech, and therefore is not protected by the First Amendment. However, employers should not immediately rely on this opinion. The case is on appeal in the 4th Circuit. Both the ACLU and Facebook have submitted amicus curiae briefs (arguments written by those not a party to the original proceeding) arguing that the district

---

15 See Donna Gurley, Social Media: Faculty and Student Rights and Responsibilities, The National Association of College and University Attorneys (June 2011)
16 Id.
17 See, e.g., City of San Diego, Cal. V. Roe, 543 U.S. 77, 80 (2004 (“a governmental employer may impose certain restraints on the speech of its employees, restraints that would be unconstitutional if applied to the general public.”). 
18 Id.
19 Id.
20 Id.; 29 U.S.C § 157.
21 Id.
22 Id.
court judge incorrectly applied the law and that the judge does not understand how users interact through SNS.

Different standards that apply in different situations mean public employers are forced to analyze the speech of its employees on many levels. Initially, public employers must determine whether the employee was acting in his official capacity or as a private citizen unrelated to his work. If the employee is acting in his official capacity, public employers must then determine if the speech relates to a matter of public concern. If so, the speech is likely protected. If not, the speech is likely not protected. If the employee was acting as a private citizen, the speech is protected unless the public employer can show that it has a strong interest in regulating the speech. Due to the complex analysis, employers are encouraged to seek legal counsel before terminating an employee for speech that might be constitutionally protected.

c. Duty to Prevent Harassment and Keep a Hostile-Free Work Environment

The rights of employees to free speech and concerted activity are counterbalanced by the duty of the employer to maintain a work environment free from discrimination, harassment, violence, and abusive behavior. Courts generally state that the location of social media outside of the workplace does not necessarily take the conduct outside of the duty of the employer to keep a hostile-free work environment. For instance, what happens when an employer learns one of its employees, acting as a private citizen, is sending threats through social media to coworkers? Or when an employer learns one of its employees uses social media to send sexually provocative images to a coworker?

Courts have stated that there is no duty for employers to monitor all electronic communications, even those produced on its system. However, courts also hold that once an employer knows (or should know) of inappropriate conduct that bears on the workplace environment, a duty likely arises on behalf of the employer to eliminate the conduct. In Delfino v. Agilent Technologies, 145 Cal. App. 4th 790 (2006), cert. denied, 522 U.S. 817 (2007), an employee of Agilent Technologies was using company computers to send cyber threats. Upon learning of the conduct, the employer immediately terminated the employee. Because of the company’s swift action, the court found the company was not liable in a subsequent civil action brought by a recipient of the cyber threats.

What is clear is that employers need not attempt to monitor all electronic communications between its employees. However, once an employer becomes, or should have become, aware of prohibited conduct, the employer should act quickly to eliminate the

---

23 Youndy C. Cook et al., The National Association of College and University Attorneys, Employers Use of Web 2.0: Take This Job and Twitter It (March 2011).
24 See, e.g., Blakely v. Continental Airlines, Inc., 164 N.J. 38 (2000) (“Thus, standing alone, the fact that the electronic bulletin board may be located outside of the workplace..., does not mean that an employer may have no duty to correct off-site harassment by co-employees. Conduct that takes place outside of the workplace has a tendency to permeate the workplace.”).
25 Youndy C. Cook et al., The National Association of College and University Attorneys, Employers Use of Web 2.0: Take This Job and Twitter It (March 2011).
26 Id.
prohibited conduct. If the employer fails to do so, it may be liable for subsequent inappropriate conduct that it could or should have prevented.

d. Making Sense of It All

Employers often face a difficult task in determining how to regulate and act upon conduct occurring over the internet and through social media in particular. Employers can feel comfortable implementing policies limiting social media access to employees during working hours. Beyond that, employers should be cautious when limiting what their employees may or may not do or say on SNS. Once an employer learns of employee activity that occurred on a SNS, the employer must consider what rights and protections that speech may be afforded before taking adverse action against the employee. Due to the often sensitive nature of conduct occurring on SNS, employers must begin investigations into suspected inappropriate conduct immediately. Regardless of the ultimate decision, employers should thoroughly document all decisions, and be sure to note the process used to arrive at that decision and all evidence considered in the decision-making process. Employers should generally seek legal counsel before terminating an employee due to conduct over the internet or through SNS.

IV. Public Records, The Ability of Employers to Search, and the Fourth Amendment

With the advancement of technology, employers often provide computers, laptops, cell phones, pagers, and other electronic devices to their employees for use in their job functions. A debate has arisen concerning the extent to which an employer can search the electronic devices and accounts it provides to its employees. For instance, if an employer provides cell phones to its employees, does the employer have unfettered access to the text messages the employee sends on that device? Can the employee read all communications sent through a work provided email address? Due to the modernity of the internet, social media, and wireless technology, many of these issues are not entirely settled. However, there are certain guidelines employers should follow.

a. Public Records Requests

Under Iowa’s Open Records Law, there is a presumption of openness for all public entities. Records of a government body are generally considered public records and must be disclosed upon request. Public records are defined by Iowa Code section 22.1(3) to include “all records, documents, tape, or other information, stored on or preserved in any medium, of or belonging to… any county, city, township, school corporation, political subdivision…”

The Iowa Supreme Court has construed the phrase “of or belonging to” in this section to mean:

A document of the government is a document that was produced by or originated from the government. Documents belonging to the government would include

---

27 Iowa Code §§ 22.1 and 22.2; Howard v. Des Moines Register & Tribune Co., 283 N.W.2d 289, 299 (Iowa 1979).
28 Iowa Code § 22.1(3) (emphasis added).
those documents that originate from other sources but are held by public officers in their official capacity. 29

The Court went on to explain that the “belonging to” determination turns on whether the public officers were acting in their official capacity as public servants and whether disclosure of the requested documents will facilitate public scrutiny of the conduct of public officers. 30 “The appropriate inquiry is whether the documents are held by the [public officials] in their official capacity.” 31

The Iowa Attorney General’s Office has issued opinions addressing the meaning of the phrase “of or belonging to” a government body. One such opinion pertains to letters, called “Board Notes,” sent from a school superintendent to members of the school board which contained the superintendent’s observations, assumptions, comments and other information on issues confronted by the school district. The Attorney General made this observation in the opinion:

Whether the “Board Notes” that you describe in your opinion request are such official documents would depend on a factual analysis of a particular “Board Notes” letter, something which is not the suitable subject of an Attorney General’s opinion. However, we note that a letter merely conveying informal observations, a draft for a speech, or background information, might be found to not constitute a “public record.”

Op. Atty. Gen. (Daggett), June 3, 1992. This opinion indicates that not every document prepared by a government official automatically becomes a public record simply because that official has created it and it exists as a record in that official’s files. The opinion is consistent with a prior opinion of the Iowa Attorney General’s Office which states:

[W]e advise that “public records” generally does include all “documents” and “records” in the possession of the public bodies identified in [the Iowa Open Records Law]. Nevertheless, we do not believe that every writing and piece of paper in the possession of a public official necessarily constitutes a record or a document. Given the definitions of these terms, we conclude that they are intended to refer to any comprehensible writing developed and/or maintained by a public body or official as a convenient, appropriate, or customary method by which the body or official discharges a public duty.


However, courts in other states have issued decisions regarding the application of public records laws to employee personal email records maintained on computer systems of government bodies. In most of these cases, the courts concluded that purely personal emails maintained on the government’s computer system were not a public record subject to disclosure. Four such cases are: Times Publishing Company v. City of Clearwater, 830 So.2d 844 (Fla. Dist. Ct. App.

29 City of Dubuque v. Dubuque Racing Ass’n, Ltd., 420 N.W.2d 450, 452 (Iowa 1998).
30 Id.
31 Id.
Times Publishing Company v. City of Clearwater, 830 So.2d 844 (Fla. Dist. Ct. App. 2002). A newspaper sought disclosure of all e-mail sent from or received by two city employees while on the job. The city allowed the employees to review and sort their e-mail into personal and public e-mail. The city provided the public e-mail to the newspaper.

The appellate court held that “private” or “personal” e-mail fell outside the current definition of public records in Florida. The e-mail was not “made or received pursuant to law or ordinance,” was not created or received “in connection with the official business,” or “in connection with the transaction of official business.” Although digital in nature, there was little to distinguish it from personal letters delivered to government workers via a government post office box and stored in a government-owned desk.

The State Ex Rel. Wilson-Simmons v. Lake County Sheriff’s Department, 693 N.E.2d 789 (Ohio 1998). Ms. Wilson-Simmons complained that other officers used the e-mail system to make racial slurs against her and brought action to compel the department to provide her with copies of the e-mail of other employees.

The Ohio Supreme Court held that the e-mails were not a “public record” pursuant to the Ohio Public Records Act because they did not document the organization, functions, policies, decisions, procedures, operations, or other activities of the department, and thus she could not have access to the records.

The Court also stated that, if it was assumed the requested e-mails constituted “public records”, Wilson-Simmons still would not have been entitled to the records. The Court stated that because this action had been brought two years after the initial request, the requested records were no longer available. The Court noted that because there was no evidence or assertion that the Sheriff’s Department violated any applicable records retention provision by writing over the records in the routine operation of its computer system, there was no violation of the law.

Tiberino v. Spokane County, 13 P.3d 1104 (Wash. Ct. App. 2000). A former employee of the County Attorney’s Office requested an injunction preventing the release of e-mails sent or received on her work computer to media companies who had requested them after she was terminated from her employment. She was terminated based on her unsatisfactory work performance, including her use of e-mail for personal matters. She threatened litigation. A newspaper reporter made a public records request for the e-mails. The employer notified the former employee that these e-mails would be provided to the reporter.

The Court held that the e-mails were public records pursuant to the Washington law since they were involved in litigation. However, the e-mails were also exempt from disclosure because their content contained nothing of public significance.

Board of County Commissioners of Arapahoe County v. Baker, Lexis 1151 (Colo. Ct. App. 2003). Under the Colorado Open Records Act (CORA), Baker (the County’s elected Clerk
and Recorder) and Sales (the Clerk and Recorder’s Assistant Chief Deputy) were directed by the trial court to release 622 of their e-mails, including 570 sexually explicit or romantic e-mails, The e-mails had been discovered pursuant to an administrative investigation conducted because a former employee had made allegations against Baker that she engaged in sexual harassment, that she created a hostile work environment, and that she had violated other laws. On appeal, Baker and Sale contended that the trial court erred in ordering the disclosure of their e-mail messages because they were not “public records” within the meaning of CORA, and that the e-mails were private, personal, and confidential communications of which disclosure was prohibited.

The Court held that the CORA prohibited the release of the “sexual harassment/hostile work environment” sub-report of the investigation, e-mails concerning the sexual harassment/hostile work environment claim, references to employees other than Baker and Sale, and the contents of e-mails relevant to Sale’s promotion, salary, overtime, and potential grounds for termination. *State ex rel. Wilson-Simmons v. Lake County Sheriff’s Dep’t*, 693 N.E.2d 789 (Ohio 1998); *State v. City of Clearwater*, 863 So. 2d 149 (Fla. 2003); *Denver Pub. Co. v. Bd. of County Comm’rs of County of Arapahoe*, 121 P.3d 190 (Colo. 2005); *Griffis v. Pinal County*, 156 P.3d 418 (Ariz. 2007); *Schill v. Wisconsin Rapids School Dist.*, 786 N.W.2d 177 (Wis. 2010); *Howell Ed. Ass’n, MEA/NEA v. Howell Bd. of Ed.*, 789 N.W.2d 495 (Mich. App. 2010); *Easton Area School Dist. v. Baxter*, 35 A.3d 1259 (Pa. Cmwlth. 2012). These cases are largely dependent upon the language of the particular public records law in question.

A recent Iowa district court opinion interpreted the scope of public records under Iowa Code Chapter 22. In *Sebring v. Des Moines Indep. Comm. Sch. Dist.*, Case No. CE71688 (Polk County Ct. 2012), the former Superintendent of Des Moines Independent Community School District, Nancy Sebring, sought injunctive relief to prevent the release of several emails after the district received multiple public records request pursuant to Iowa Code Chapter 22. The emails, sent by Sebring during working hours through her public email account, contained sexually charged language. Sebring argued that the emails were not public records because they were not created by her in her official capacity as Superintendent, and alternatively that release of the emails would cause substantial and irreparable harm to her and the recipient. However, the district court concluded that the emails were records “of or belonging to” the government and, after determining that the potential harm to Sebring through release of the records was outweighed by the public interest in transparency of government, ordered the release of the emails.

The *Sebring* opinion was seemingly against the trend of courts in other states mentioned in this paper.

So what should employers do? Public officials confronted with a public records request that involves public employee use of email or text messages should (1) determine what records may be available which are responsive to the request; (2) review each available record individually and determine whether the record is a public record (that is, is the document held by public officials in their official capacity); and, if so, (3) determine whether that record is nevertheless confidential under the law. Due to the complexity of the analysis and the need to determine each request on a case by case basis, public officials should consent with legal counsel regarding these matters.
b. The Fourth Amendment

The Fourth Amendment provides: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…” The Fourth Amendment applies when the government acts as an employer. Thus, public employees are entitled to certain protections against unreasonable searches and seizures by their employers.

In *City of Ontario v. Quon*, the Supreme Court of the United States addressed for the first time the extent to which public employers could search electronic devices they provided for their employees. In that case, the City of Ontario (“the City”) provided pagers to its police officers. The officers were given a strict text message limit per month. The City made clear to the officers that there should be no expectation of privacy in any of the text messages sent or received. After realizing that officers were often going over the text message limit each month, the City decided to investigate whether there was a need to raise the monthly text message limit. In its investigation, the City looked at the text messages sent by each officer over the course of a two month period to determine whether the text messages were sent by the officers in their official capacities. When investigating the plaintiff’s text messaging history, the City redacted all messages sent or received by the plaintiff during nonworking hours. The City learned that on an average shift the officer sent or received 28 personal text messages and just 3 related to police business, and that many of the messages were sexual in nature. The plaintiff was subsequently disciplined by the City.

The plaintiff then brought suit against the City, alleging a violation of his Fourth Amendment rights against unreasonable searches and seizures. Upon granting certiorari, the Supreme Court of the United States held that, even assuming that the plaintiff had a reasonable expectation of privacy and therefore protection under the Fourth Amendment, the search did not violate the plaintiff’s Fourth Amendment rights. The Court reached this decision due to an explicit exception that a search by a government employer conducted for a “noninvestigatory workplace purpose[e]” is reasonable if it is justified at its inception and the measures adopted are reasonably related to the objectives of the search.

The Court expressly did not provide guidance on whether public employees had a reasonable expectation of privacy in its communications on government owned devices or whether public employers could conduct warrantless searches of messages on those devices. Accordingly, public employers should be careful in conducting warrantless searches even on devices owned by the employer, as the *Quon* opinion indicates that those searches may (or may not) be a violation of the Fourth Amendment rights of its employees.

One key determination courts often use in determining the scope of the Fourth Amendment is the amount of privacy the individual bringing the claim could reasonably have

32 U.S Const. amend. IV.
34 *City of Ontario, Cal. V. Quon*, 130 S.Ct. 2619, 2627 (2010).
expected.\textsuperscript{35} For example, a public employee who is repeatedly told that emails sent or received through his work provided email address are public and that he should not expect any privacy whatsoever in those emails will probably receive less Fourth Amendment protection than a public employee who was not so informed. Accordingly, public employers should clearly and continuously notify their employees that they should not expect privacy in their communications, whether through email, text message, or otherwise. In addition, public employers should require that all of their employees sign a consent form acknowledging that they have been notified not to expect any privacy whatsoever in communications stemming from their work devices or accounts.

c. Computer Use Policies

Employers that provide computers to employees to perform any aspect of their jobs must have a computer use policy in order to protect their ability to monitor the use of their computer system and to enhance their ability to conduct a lawful search of electronic technology used by employees.

The first element of any policy is notice to employees such as the following

\textbf{Notice}

All of the Employer’s automated and electronic systems, including the computer system, email, voice mail, Internet access, electronic storage systems, are property of the Employer. The Employer has the right to access, inspect, review, copy, modify, and delete any information transmitted through or stored in any of its systems. To the extent that any computer or electronic communication activities are regulated by state or federal law, the Employer will observe all such regulations imposed upon it. If the Employer conducts an examination or inspection under the terms of this notice, there will be at least two individuals present at the time of the examination or inspection.

Many employers have an extensive computer use policy. A sample policy is attached at the end of this paper. The policy statement should be reinforced with consent statement in which the employees acknowledge that they understand and agree to comply with the policy:

\textbf{Consent}

I hereby certify that I have read and fully understand the contents of the Employer’s Electronic Systems Policy. I acknowledge that the Employer reserves the right to modify or amend its policies at any time, without prior notice. My signature below certifies that I have received notice of the Policy, that I accept the terms of the Policy, and that I consent to be governed by and adhere to the terms of the Policy as a condition of my continuing employment.

\textsuperscript{35} Id. at 2631.
Because employees now frequently use their own electronic devices, it is important for employers to have a policy in place with regard to the use of privately-owned technology. Here is a sample policy statement:

Non-Employer Resources: During the employee’s working hours, the use of employee-owned computers and electronic devices, whether accessed via the Employer’s System or otherwise, is subject to the Employer’s Electronic Communication Policy. This includes, but is not limited to, access to the Internet, communication on personal webpages, transmission or receipt of e-mail messages, blogging, instant messaging, use of regular and cellular phones, voicemail, and/or text messaging.

Finally, employers need to control their identity and to regulate who speaks for them. And employees need to be specifically advised that they may not speak on behalf of the employer unless they are authorized to do so. The following is a sample attribution policy statement:

Attribution: The Employer has designated employees who may publicly communicate on its behalf. Employees who are not designated to do so may not communicate on behalf of the Employer or make any statements that are attributed to the Employer. When employees post messages to electronic posting forums or blogs on the Internet using the Employer’s System, the messages must contain a disclaimer at the end of the message that states: “The opinions expressed in this message are mine only, and do not reflect the opinion or position of my employer.” When employees post messages to electronic posting forums or blogs on the Internet and identify themselves as employees of the Employer, the messages must contain a disclaimer at the end of the message that states: “The opinions expressed in this message are mine only, and do not reflect the opinion or position of my employer.”

V. “Friending” Employees

Whether or not supervisors should become “friends” with their subordinates is a tricky question. On one hand, the supervisor may be close friends with a subordinate, or may wish to monitor the public disclosures the employee makes about the company. On the other hand, employers who have “friended” their employees are in a difficult position to assert that they did not have access to protected information on the employee’s social media page.

Suppose a person responsible for all human resources decisions “friended” an employee of the company on Facebook. Sometime later, the employee posts on his Facebook page that he is homosexual. Now imagine the employee shows up to work late two days in a row the following week, and the employer decides to terminate him. Even if based on legitimate business reasons, the employee may feel that he was discriminated against for revealing himself as a homosexual.

---

36 Youndy C. Cook et al., The National Association of College and University Attorneys, Employers Use of Web 2.0: Take This Job and Twitter It (March 2011).
Employees may also feel coerced into accepting a “friend” request from a supervisor. Imagine, for instance, that you are a new employee and your boss requests to be your “friend” on Facebook. As the subordinate, you wonder what your boss might think if you deny his request. Even if you do not want to be “friends” with your boss, you may feel that you have no choice but to accept his “friend” request in order to remain in good standing with your superior.

Additionally, employers may face an increased duty to affirmatively act by “friending” its employees. An employer’s duty to act to prevent harassment or discrimination begins when the employer knows or should have known about prohibited behavior. If the supervisor of an employee is “friends” with the employee on Facebook, and the employee is discriminated against on Facebook, the employee will have an easier time proving that the employer knew or should have known of the discriminatory behavior. On the other hand, “friending” employees may provide the employer with greater ability to monitor and prevent prohibited conduct. Certainly, employers want to limit discrimination and harassment. However, the risks may outweigh the benefits. Employers who are unable to consistently monitor SNS are unlikely to catch all prohibited conduct. Imagine the employer who takes action against one instance of discriminatory conduct through SNS, but fails to realize that a separate instance of harassment is also occurring on the same SNS. The victim of the second instance may be able to show that the employer should have known of the discriminatory conduct since it knew of the other incident. While employers should never turn a blind eye to discrimination or harassment, if the employer is unable to consistently monitor SNS to ensure that discrimination does not happen, it may be unwise for the employer to create access to those channels of information to begin with.

A competing interest weighing in favor of “friending” employees is the desire of the employer to monitor its confidential and proprietary interest. Often, former employees will use Facebook to reach out to former clients in an effort to entice them to switch to their the new company of the employee. Several cases have held that evidence of violations of non-compete agreements obtained through SNS is admissible in court. Employers with a particularly strong interest in enforcing non-compete covenants and in protecting its proprietary information may find that the benefits of “friending” employees outweigh the risks.

VI. Employer’s Presence on Social Media Sites

Social networking sites may be used by organizations to provide information to the public, and cities are increasingly creating their own pages on such sites in order to facilitate the exchange of information.

The most common concern that arises in this area is the extent to which the city may regulate the messages which are posted by others on its social networking page. Persons posting messages on the city’s social networking page are protected by the First Amendment. The ability of the city to regulate the messages posted by others turns on whether the page is a traditional public forum, a designated public forum, or a nonpublic forum under First Amendment principles.

37 Id.
38 Id.
If the page will be open to messages posted by any other users on any subject, the page is likely to be considered a space that is intentionally opened by the city to expressive activity and which is not limited to a particular type of speaker or speech, or an “unlimited designated public forum.” In an unlimited designated public forum, the city’s ability to restrict speech is the most circumscribed. A content-based restriction on speech must be necessary to serve a compelling government interest and be narrowly drawn to achieve that interest. Particular viewpoints cannot be favored.

No constitutional problem arises from the prevention and punishment of certain well-defined and narrowly limited classes of speech, including defamation, incitement to a breach of the peace or imminent lawless action, threats, obscenity, and words which by their very utterance inflict injury or tend to incite an immediate breach of the peace.

The rules of operation of the social networking site may also speak to the regulation of content posted by other users. Therefore, the city may take actions to regulate the posting of content by users consistent with the social networking site’s rules of service and in accordance with First Amendment principles, including the removal of prohibited content from the page. Prohibited content may include speech which is defamatory, contains threats, or is obscene.

For cities that maintain a presence on SNS, here are few practice tips: (1) research and comply with the rules of operation of the social networking sites, (2) give notice to all users that the messages or other content posted on the city’s page by users do not necessarily represent the views of the school district, and that the city may take actions to regulate the posting of content by users as appropriate, (3) when regulating such content, consider the type of user (i.e., employee or member of the general public) and the type of speech involved in order to determine the application of the proper First Amendment standard, and (4) in the event that the city takes action against a user, it should remember to preserve any relevant evidence.

VII. Fair Labor Standards Act Issues

Employees who are covered by the Fair Labor Standards Act (this includes most city employees) are required to be paid for all hours that they work, regardless of whether that work is performed while they are physically on the employer’s premises. Employees are also required to be paid for all work which an employer “suffers or permits” them to perform that is of benefit to the employer.

In combination, these two concepts mean that employees who use computers or cell phones to perform work-related functions while they are away from the job and who do so during hours of the day when they are not scheduled to work are entitled to be paid for the time that they spend performing work-related functions. These work-related functions could be as simple as checking work-related emails, text messages, or voice mail messages or it could be as complicated as preparing business agreement documents for a multi-million dollar project in which the city is involved. If the amount of time spent by employees working outside of their regular hours is so small or insignificant (de minimis) that it cannot practically be recorded for payroll purposes, it need not be counted as hours worked. The periods of time must be uncertain and indefinite. See 29 C.F.R. § 785.47.
Employers need to be aware of their potential liability for work performed “off-the-clock” because the U.S. Department of Labor (which enforces the Fair Labor Standards Act) has determined that it will take a more aggressive posture in resolving wage and hour complaints and will insist upon the payment of liquidated damages (an amount equal to the back pay owed to employees) in the settlement of alleged violations of the FLSA. To protect themselves, employers need to adopt a policy which specifically addresses the use of electronic technology by FLSA-covered employees during hours of the day when they are not scheduled to work.
Policy

For the purpose of this policy, a "computer" is any device that sends or receives data transmissions, data files, or electronic messages generated on or handled by electronic communication networks, personal computer systems, centralized computer systems, or software owned by the City. This policy also covers personal equipment (such as items purchased with an employee's personal funds or brought into the environment by the employee) that is connected to the City's computer network or systems. For purposes of the Employee Handbook, the term does not apply to the use of the library's patron computer network.

Computer systems and Internet access are provided by the City to support open communications and exchange of information, as well as to provide the opportunity for collaborative City-related work. The City encourages the use of electronic communication devices by its employees. Like any resource available to employees, personal use of the Internet is a revocable privilege. The use of City-provided computer systems must be for City business and not for personal business, except as allowed in the policy.

The computer systems’ hardware and software are the property of the City. All messages sent or received, and all information stored on the City’s computer systems are the property of the City and not the private property of any employee.

An employee’s personal use of City-owned computer systems is a privilege, not a right. An employee is solely responsible and shall be personally liable (legally, financially, or otherwise) for the employee’s use of City-owned computer systems outside the scope of the employee’s employment.

Because no one controls the Internet, having an e-mail account will likely result in the employee’s receipt of spam, including messages that may contain highly offensive and sexually explicit content. Even though the City uses various automated mechanisms in an attempt to keep spam or objectionable material from employee's mailboxes, the City does not guarantee that all objectionable material will be identified or stopped. Users of the City e-mail systems are expected to make a reasonable individual effort to attempt to identify potentially objectionable content before opening an email item that they may find offensive.

Guidelines

The following are guidelines regarding computer, e-mail, and Internet usage:

- Employees must use the Internet in a professional and ethical manner.
- Employees must not use electronic communication devices for harassment or other inappropriate behavior regarding race, color, creed, religion, sex, sexual orientation, gender identity, ancestry, national origin, age or disability.
- Employees must not use electronic communication devices to create, access, display, archive, store, distribute, transmit, edit or record material which is sexually explicit, immoral, obscene, threatening, defrauding, violent or unlawful.
- Employees must not create, distribute, copy, or knowingly use unauthorized copies of copyrighted material or software, store such copies on City computers, or transmit them over the City’s networks.
- Employees must use the Internet only to access information that is publicly available or to which the employee has authorized access.
- Employees must not use electronic communication devices for illegal activity.
- Confidential or sensitive information should not be transmitted over the Internet without appropriate security measures taken to safeguard the information.
- Contacts made over the Internet should not be entrusted with confidential City information unless a due diligence process has first been performed. Users shall not place City material (such as software, internal memos, and so forth) on any publicly accessible Internet computer, unless the posting of these materials has first been approved by the appropriate department director.
- Credit card numbers, SCAN numbers, telephone calling card numbers, logon passwords, and other parameters that can be used to gain access to goods or services, must not be sent over the Internet in an unsecured form. The City cannot guarantee confidentiality over the Internet. Therefore, individuals entering personal information (such as credit card numbers, social security numbers, and so forth) for personal use do so at their own risk.
- Exchanges of software between the City and any third party shall not proceed unless permission has been received from the department director and the Information Technology Director.
- The truth or accuracy of information on the Internet and in e-mail should be considered suspect until confirmed by a reliable source.
- To avoid libel, whenever any affiliation with the City is included with an Internet or internal e-mail, message, or posting, “flaming” or similar written attacks are strictly prohibited. Whenever staff members provide an affiliation, they must also clearly indicate that the opinions expressed are their own and do not reflect those of the City.
- Users shall not use another user’s e-mail account without permission of the account’s owner. Unless specifically acting as an agent for another when sending a message from another account, users should clearly identify themselves as the author of the e-mail message.

**Limitations**

The following are limitations regarding personal use of the City's computer systems:

- Use must not interfere with the performance of the employee’s duties or productivity.
- Use is of nominal cost or value.
- Use must not negatively impact the performance of the City’s computing infrastructure or the system/device being used.
- Use must not interfere with the intended function of the device being used.
- Use must not create the appearance of impropriety.
- Use is reasonable in time, duration, and frequency.
- Use makes only minimal use of hardware and software resources.
- Use must not reflect poorly on the City or its reputation.
Software Usage

It is the City’s policy to respect all computer software copyrights and to adhere to the terms of all software licenses to which the City is a party. Unauthorized duplication of software may subject users or the City to both civil and criminal penalties under the United States Copyright Act. City employees may not use software in any manner inconsistent with the applicable license agreement, including giving or receiving software or fonts from contractors, citizens, and others.

The purchase of all commercial software to be installed on City-owned computers will be coordinated or purchased by the Information Technology Department.

Shareware© software is copyrighted software that is distributed via the Internet. It is the policy of the City to pay Shareware authors the fee they specify for use of their products. Under this policy, acquisition and registration of Shareware products will be handled the same way as for commercial software products.

Users are not permitted load or download any personal software onto City computers. Generally, City-owned software cannot be taken home and loaded on a user's home computer if it also resides on a City computer. If a user is to use software at home, the City will purchase a separate package and record it as a City-owned asset, unless the software company provides in its license agreements that home use is permitted. If an employee must use City-owned software at home, each user must consult with the Information Technology Director to determine if appropriate licenses permit home use.

Employees shall only access or use information they are authorized to obtain or utilize. Employees who discover a violation of any part of this policy must immediately notify their department directors and the Information Technology Director, who will in turn inform the City Manager. Misuse of the City’s computer systems can be grounds for disciplinary action, up to and including termination of employment.

Users of the City’s information systems or the Internet should realize that their communications are not automatically protected from viewing by third parties.

At any time and without prior notice, the City reserves the right to examine e-mail, voice mail, personal file directories, and other information stored on or transmitted through City computers. An employee’s use of the City’s computer systems or electronic technology constitutes consent to such examination.

City employees or volunteers cannot establish Internet or other external network connections that could allow non-City users to gain access to City’s systems and information.

Alternate Internet Service Provider (ISP) connections to the City’s internal network are not permitted unless expressly authorized by the City Manager and the Information Technology Director and properly protected by a firewall or other appropriate security devices.
Whenever passwords or other system access control mechanisms are lost or suspected of being stolen or disclosed, the Information Technology Director must be notified immediately. All unusual behavior (such as missing files, frequent system crashes, misrouted messages, and so forth) shall be reported immediately to the Information Technology Director.

All use of the Internet must be in full compliance with U.S. Copyright Laws. Unless otherwise noted, all software on the internet should be considered copyrighted work. Therefore, employees are prohibited from downloading software or modifying any such files without permission from the copyright holder.

Any infringing activity by employees may be the responsibility of the City. Therefore, the City may choose to hold employees liable for their actions.

Files which are downloaded from the Internet must be scanned with virus detection software before installation or execution. All appropriate precautions should be taken to detect for a virus and, if necessary, to prevent its spread.

The introduction of viruses or malicious tampering with any computer system is expressly prohibited. Any such activity will result in disciplinary action, and, if it is a violation of state or federal law, it will also be prosecuted.

Sending or receiving of large files (larger than 50 megabytes) through the City’s Information Technology systems is generally discouraged and may be restricted at the firewall, e-mail gateway, or e-mail server in order to protect the system and the IT infrastructure. The use of Streaming Media sites is generally discouraged and may be restricted at the firewall in order to protect the IT infrastructure. Exceptions to this policy will be reviewed case-by-case by the Information Technology Director. Alternatives to file transmission through e-mail may be recommended or required depending on the situation.

**Social Computing Guidelines**

The purpose of this policy is to establish City regulations defining the use of various technologies known collectively as “social media”. Social media accounts shall be used for the purpose of informing the public about city business, services, and events. All official City presence on social media accounts are considered an extension of the City’s information networks.

This policy covers all social media messages generated on or handled by electronic communication systems owned by the City. This policy is also applicable to all social media messages generated by employees of the City that relate to their status as an employee of the City. The regulation of employee speech is subject to the right of employees to freedom of speech as that right has been interpreted by the court.

The City’s website will remain the official location for content regarding city business, services, and events. Whenever possible, links within social media formats should direct users back to the City’s website for more information, forms, documents, or online services necessary to conduct
business with the City.

All City social media accounts should be viewable to the public and not use privacy settings.

The City logo and authorized departmental extensions should be used on all social media accounts to confirm authenticity of site.

If a department chooses to participate in social media, online representation on social media accounts is ultimately the responsibility of the Department Director. The Department Director shall appoint a social media moderator to control the social media account and ensure appropriateness of content.

Departments should regularly monitor and update accounts at least twice a week.

Employees representing the City via social media accounts must conduct themselves at all times as representatives of the City and must comply with the Guidelines contained in this policy and with the provisions relating to “Prohibited Content”.

Any employee who discovers a violation of this policy shall immediately notify their Department Head who shall in turn inform the City Manager. An employee who violates this policy or uses social media for improper purposes shall be subject to disciplinary action up to, and including, termination of employment.

Definitions

Social Media: Various forms of discussion and information-sharing, including social networks, blogs, video sharing, podcasts, wikis, message boards, and online forums. Technologies include: picture-sharing, wall-postings, fan pages, email, instant messaging, and music-sharing. Examples of social media applications include, but are not limited to, Google and Yahoo Groups (reference, social networking), Wikipedia (reference), MySpace (social networking), Facebook (social networking), YouTube (social networking and video sharing), Flickr (photo sharing), Twitter (social networking and micro-blogging), LinkedIn (business networking), and news media comment sharing/blogging.

Business Purposes: Use of social media as a means of communicating official information about the City, including events, department activities, emergency information, and feature stories. Business Purposes also includes use of social media for interaction with a professional association, information source necessary to the job duties of an employee, and interaction with other members of a professional association.

Personal Use: On-duty and off-duty use of personal social media sites by a City employee for any purpose that is not a business purpose. This includes access on personal or City provided computers and smart phones.
Posting Guidelines

Employees should be conscious of what they post on social media sites and avoid presenting personal opinions that imply endorsement by the employee’s Department or the City. If posted material could be attributed to the employee’s Department or the City, the post must be accompanied by a disclaimer identifying the statements or opinions presented as those of the poster and stating that the statements or opinions do not reflect those of either the employee’s Department or the City.

Employees should not portray themselves as spokesperson for their Department or the City unless they are specifically authorized to do so by either the Department Head or the City Manager.

Departments that use social media accounts are responsible for complying with applicable federal, state, and local laws, regulations, and polices. This includes adherence to established laws and policies regarding copyright, records retention, Freedom of Information Act (FOIA), First Amendment free speech rights, privacy laws, and information security policies established by the City.

Employees may not post text, video, pictures, or other material that would reasonably be considered to be detrimental to the image of the City or of an individual Department. Only post material which you have permission to use.

Employees should keep in mind that once an item is posted it is publicly available on the Internet and cannot be retracted.

Prohibited Content

The following content shall be prohibited on official City social media sites.

- Profane language or content
- Content that promotes, fosters, or perpetuates illegal discrimination of any kind.
- Sexually explicit content or links to such content.
- Solicitation of others for commercial ventures, or religious, social, charitable or political causes.
- Making or publishing of false, defamatory, or malicious statements concerning any employee, supervisor, the City, or its operations.
- Personal information about employees.
- Posting of HIPPA protected information is not permitted.
Use of chat sessions in social media will not be permitted.

The City Manager, or designated representative, reserves the right to delete submissions that are deemed inappropriate, according to prescribed unacceptable content standards. If any record is deleted for unacceptable content, it is the responsibility of the affected Department to retain a public record of that content and keep a record of why the information was removed.

Friends, fans, or followers should be removed if they continue to post inappropriate content. One warning should be given. If the individual posts inappropriate content a second time, they should be removed or blocked.

**Social Media Account Security**

Department social media accounts should be tied to a City email address.

Moderators should never leave a workstation unattended when logged on the social media account.

Only the Department Director and moderator(s) should know the login and password to social media accounts.

If the moderator changes, the login and password should also change.

**Personal Use of Social Media**

Employees should make certain any online activities do not interfere with their effectiveness at work and ensure any on-duty personal use is limited in nature. If on-duty personal use is interfering with work effectiveness, employees will be subject to disciplinary action.

Employees should be mindful of blurring their personal and professional lives when using or accessing social media sites.

Employees may not use social media to engage in libelous, defamatory, obscene, or maliciously false behavior directed at the City, Departments, elected officials, appointed officials, other employees, or members of the public.

Employees may not post confidential information which they have learned through their employment with the City.

Posting of HIPPA protected information is not permitted.

Employees may not use their City email account in connection with a personal social networking account.

Employees shall not participate in online social media or forums on behalf of the City or
their Department unless they are authorized to do so by the City Manager or their Department Director.

When violations of these guidelines occur, the City reserves the right to exercise judgment in determining the appropriate level of discipline by reviewing each incident on a case-by-case basis.