SUMMIT LAW GROUP
a professional limited liability company

Legal Ramifications of the Social Media Explosion: *An Employer's Guide*

30th Annual Labor Relations Institute

April 28-30, 2010

Kristin D. Anger
Sofia D'Almeida Mabee

Summit Law Group
315 Fifth Avenue South
Suite 1000
Seattle, WA 98104
(206) 676-7000
kristina@summitlaw.com
sofiam@summitlaw.com

I. INTRODUCTION

The explosion of social media in recent years has changed the way people communicate with one another. This phenomenon also blurs the lines between our professional and personal lives in ways that create a range of legal issues for employers. While it is difficult for employer policies and practices to keep pace with the rapidly-evolving technology (and the behavioral issues that come with it), it would be unwise for an employer to bury its head in the sand and assume that social media is a passing fad. Rather, employers should understand the emerging legal issues regarding the impact of social media on the workplace and update policies and practices to address those issues.

These materials provide an overview of the primary legal issues for employers arising from social media. In a nutshell, the term "social media" encompasses web-based technology that facilitates social networking and communication. It is instantaneous and unedited. Social media includes blogging, micro-blogging (Twitter), audio-visual networking (YouTube), and social networking (Facebook, MySpace.) Text messaging and instant messaging present similar issues, and are also addressed in these materials. Topics addressed include the use of social media in hiring, employee misconduct associated with social media, employer liability issues arising from social media and steps employers should take to minimize that liability and potential employee misconduct.[1]

II. LEGAL ISSUES

A. Employer Use of Social Media in Hiring.

Never before have employers had access to so much information about job applicants. Through a few clicks of a mouse, you can often find all kinds of information about an individual. From a Facebook profile, for example, you might learn about the individual's friends and family members, club memberships and professional affiliations, religious beliefs, sexual orientation, recreational activities, etc. Some of this information might provide valuable insights into an applicant's background, judgment and professionalism that simply cannot be gleaned from the applicant's résumé or interview. Because of this, many employers have begun checking applicants' social media profiles during the hiring process, and there have been a multitude of news stories about people who have lost out on job opportunities because of inappropriate content posted on their social media sites. While employers may well be tempted to take advantage of these informational tools, employers should understand and take steps to minimize the risks associated with this approach in hiring.

[1] It is worth noting what these materials do not address as well. Many public sector agencies are taking advantage of social media to connect with constituents. Some, for example, have their own Facebook pages, and as part of their jobs, employees engage in blogging or use Twitter to communicate on matters of public concern. There are a number of legal issues that arise from these efforts, including public records retention, compliance with the Open Public Meetings Act, etc. Those issues are beyond the scope of these materials, which focus more specifically on employment matters. There is, however, a wealth of information available to agencies that want to pursue their own official social media sites or communications. A good resource for information on this topic is the Municipal Research Service Center website (www.mrsc.org), which has links to relevant articles and other guidance.

1. What are the Risks of Using Social Media Sites in Your Hiring Process?

a. Discrimination Claims. State and/or federal laws prohibit discrimination on the basis of factors such as an applicant's or employee's race, gender, age, religion, marital status, military status, disability, sexual orientation, and genetic information. As a result, employers are advised to be cautious about what information they seek from an applicant during the hiring process. Employers should steer clear, for example, from questions about whether an applicant is married, whether and where he or she goes to church, how old the applicant is, and any other question that relates to a protected status. As an employer, if you don't have this information in the first place, you cannot be liable for having relied upon it in making a hiring decision. But if an employer accesses an applicant's Facebook or MySpace profile, the employer could learn a wealth of information about an applicant that should not properly be considered in making a hiring decision. If the employer does not ultimately hire the applicant, he or she could assert a discrimination claim that the decision was based on a protected status.

b. Privacy. If an applicant's social media site is publicly available, then he or she would have a very difficult time asserting that an employer's actions in accessing the site violated his or her privacy rights. In some cases, however, employers have used employees or other contacts to access sites that are not generally accessible to the public. Depending on the circumstances, doing so could create some legal exposure.

c. Misleading or Inaccurate Information. Obviously, not every piece of information available on the Internet is accurate. A savvy job hunter may have persuaded dozens of social friends to provide glowing endorsements on LinkedIn, even though the friends have had no professional dealings with the individual. By automatically accepting online information as authentic and reliable, an employer risks making poor hiring decisions.

d. Fair Credit Reporting Act. The FCRA requires that if an employer retains a third party to conduct a background check on an applicant, certain procedural protections must be afforded, including the applicant's authorization of the background check and, if adverse information is used to deny employment, notice to the applicant of his/her right to obtain the report. To the extent an employer uses a background checking agency that accesses social media sites, it must ensure that FCRA requirements are observed.

2. Steps to Minimize Liability.

a. Have a Lawful Reason for Rejecting a Candidate. If you use social media sites to evaluate job applicants, ensure that you can articulate a non-discriminatory reason for rejecting an applicant. This is always a good idea, but it becomes particularly important if you have viewed an applicant's social media profile and have learned all kinds of information that should not lawfully be considered in making a hiring a decision. Absent the social media site, you likely would not have had this information, and therefore could not be liable for using it in making a hiring decision. But once you have the information, an applicant can assert that you improperly relied on it to reject him or her. Accordingly, it is even more important to have a legitimate, nondiscriminatory reason unrelated to the applicant's protected status for rejecting the applicant.

b. Focus Only on Job-Related Information. Just as in a job interview setting, an employer should disregard information that is not job-related and focus on the information that reflects on an applicant's ability to do the job for which he/she applied. Obviously, some information can fall into a gray area – dozens of photos showing the applicant in various states of inebriation and undress may not reflect how the applicant would perform specific job duties, but those photos may very well reflect on whether the applicant has the judgment, discretion and maturity needed for the job.

c. Consider Having Someone Filter Social Media Content to Ensure Decision Makers Have Only Job-Related Information. If you use social media sites to research applicants, it may be worthwhile to have someone who will not be a decision-maker in the hiring process conduct this research. That person can filter out information that should be irrelevant (*e.g.*, church affiliations, sexual orientation) to ensure that decision-makers only have job-related information in deciding whom to hire. This could be helpful in defending against a discrimination claim, as the decision-makers could not rely on improper information if they did not have that information.

d. Ensure That Information Is Authentic and Reliable. Do not rely on social media content exclusively to vet job applicants. Consider the reliability of the source, especially if you are looking at what third parties are saying about the candidate.

e. Use a Consistent Approach. If you decide to use social media sites in your hiring process, make sure that you do so consistently for all applicants. For example, check the same sites for all applicants (or all applicants who make it to a particular step in the hiring process) and document your efforts.

f. Ensure That FCRA Requirements Are Met. If you retain a third party to check applicant backgrounds, including by checking social media sites, ensure that FCRA's procedural requirements regarding consent and notice are satisfied.

B. New Forms of Employee Misconduct.

1. Sexting and other forms of harassment via technology.

Think sexual harassment and text messaging. Sexting occurs when an employee uses text messaging to send sexually explicit messages. Sexual harassment might also occur through postings and material on social media sites, such as Facebook. A good policy and employee training can go a long way toward eliminating sexting and other forms of harassment via new technology.

2. Defaming co-workers on the internet.

Employees who are not happy at work now have a new medium to communicate that displeasure: the internet. Blogging, instant messaging, and postings on social networking sites act as a form of "virtual bulletin board" giving employees the ability to vent discontent to a large audience instantly. Unfortunately, venting can turn into defamation or violate other workplace rules.

3. Conduct Unbecoming.

Social medical postings give employees the ability to write words, post pictures and videos, and create links to other websites and pages. An employee's social media postings can turn into "conduct unbecoming" of the employee's official duties when the postings undermine the employer's reputation and its ability to serve the public. For example, a teacher who posts sexualized photographs of minors.

4. Virtual chatting.

Chatting at work is not a new problem, but it has taken on a new virtual form that can be difficult to control and leads to losses in productivity.

5. Releasing confidential information.

Employees have access to a variety of sensitive information in the workplace, including medical information about other employees, discussions in executive session, legal advice, and information about pending internal investigations. An employee's release of confidential information can happen deliberately, through a text or instant message, or it can happen inadvertently. For example, a manager might update his Facebook status to read, "I hate firing people." Someone who knows the

manager's schedule might be able to piece together who had been asked to leave.

6. Publicized Misuse of Sick Leave.

Sometimes employees call in sick when they are not, in fact, sick. With the arrival of social media, employers may see pictures of an employee at a Mariners game on a day the employee called in sick.

C. Off-Duty Conduct.

Generally, employers are not entitled to discipline employees for off-duty conduct. However, discipline is allowed if the off-duty conduct has a "nexus" to the employee's job. The following are some examples.

- When an employee's off-duty conduct affects the employee's ability to maintain satisfactory and productive working relationships with co-workers, discipline can be appropriate. An example of this is an employee who maliciously defames a co-worker in an online blog.

- A second exception to the general rule involves off-duty conduct that undermines the employer's reputation and its ability to serve the public. For example, a police officer who identifies himself as an officer in a video posted on the internet that contains racially derogatory statements.

- A third exception would involve the employee's release of confidential employer information. For example, a human resources employee who sends text messages after work revealing another employee's medical diagnosis.

- A fourth example would be the misuse of employer equipment. For example, an employee who takes home an agency laptop and downloads large quantities of data for personal use in violation of the agency's computer use policy.

D. New Areas of Employer Liability.

1. Failure to Control References.

To reduce the risk of defamation claims, many employers maintain policies providing that all reference inquiries for current and former employees should be directed to Human Resources (or the appropriate member of management). This ensures that the employer has control over the content of the reference information provided, and permits the employer to take advantage of the state statute limiting civil liability for employment references, which imposes certain requirements. Social media sites afford employees with a new means of providing references, however. LinkedIn, for example, is a professional networking site through

which individuals can establish connections with other users. The site allows users to recommend other professionals and comment on their skills and experience. It is not uncommon for users to request that others post recommendations, which the users can then rely on for business development or in a job search. Other social networking sites can also be used to post commentary about professional acquaintances.

While employers may not be terribly concerned about these kinds of recommendations because they are typically positive (given that employers are more often concerned about liability arising from negative references), these references are not without risk. For example, assume that the employer has terminated an employee for poor performance and the employee has sued the employer for discrimination. The employer may be able to obtain dismissal of the suit on summary judgment where there is clear evidence establishing the poor performance. But what if the employee had persuaded a manager to post a recommendation on LinkedIn? That positive recommendation by a manager could undermine the employer's position in the lawsuit and could even be enough to prevent summary judgment. Alternatively, if a manager posted something that was highly critical of a former employee, the employer could potentially be liable for any harm suffered by the former employee. These internet-based recommendations can create the same kinds of liability as traditional references, but we do not tend to think of them the same way or subject them to the same policy requirements.

2. Defamation/Harassment.

Employees at work may access personal social networking sites and post defaming or harassing communications that harm third parties, who then blame the employee's employer. Generally, employers are not liable for the actions of their employees unless those actions fall within the scope of the employee's employment. Intentional illegal acts are generally not considered within the scope of an employee's employment. However, even if an employee's actions do not fall within the scope of his or her employment, an employer could be liable if it knew about the harassment or defamatory postings and failed to stop it.

3. Violation of trademark/copyright/patent laws.

An employee's violation of trademark, copyright, or patent laws at work by posting photographs, published works, or video clips owned by someone else can also present legal risk to the employer if the employee's actions fall within the scope of his or her employment or the employer knows about the violations and fails to stop them. Employers should maintain and enforce policies requiring compliance with trademark, copyright, and patent laws.

4. New sources of evidence of discriminatory motive.

An employee subjected to an adverse action such as a demotion or termination might look for evidence that the action was discriminatory or retaliatory on her manager's blog or social networking site. For example, a female employee terminated for misconduct might look for evidence on her manager's social networking site to support a claim that the manager was motivated by a bias against women. Additionally, a manager who becomes "friends" with a subordinate on a social media site may learn information about the subordinate's protected status that the manager otherwise would not know, such as that the subordinate has a disability, belongs to a certain religious group, or is gay. If the subordinate is subsequently disciplined or discharged, he/she could assert that the action was based on his/her protected status and that the manager knew of the protected status via the social networking site.

E. Legal Pitfalls to Avoid When Investigating and Disciplining Based on an Employee's Use of Social Media.

1. The Fourth Amendment.

Unlike private employees, public employees are protected by the Fourth Amendment to the US Constitution from searches by their employer that invade their "reasonable expectation of privacy." The U.S. Supreme Court is going to be determining the boundaries of that right in a case currently pending before it: *Quon v. Arch Wireless Operating Company, Inc.*, 529 F.3d 892 (9th Cir. 2008).

The case involves text messages sent and received by police officers that were sexually explicit and personal in nature. Although the police department formally prohibited personal use of the pagers, it informally allowed it. The Ninth Circuit Court of Appeals sided with the officers, finding that the public employer violated the officers' Fourth Amendment rights because they had a "reasonable expectation of privacy" in the messages.

The US Supreme Court's decision in *Quon* may overturn this decision or it may affirm it. In either case, the decision will provide further guidance on the limits of public employees' Fourth Amendment rights in the world of social media.

2. Right to Privacy.

Washington State recognizes that individuals have a right to privacy in certain information about themselves. This can include medical information or information about one's personal sexual life. When investigating an employee for misconduct relating to social media, employers should be careful to limit the scope of the investigation to what

is necessary and relevant. The same applies to monitoring employees' postings on social media sites: employers should normally limit themselves to what is publicly available and relevant to the employee's job.

3. Federal Telecommunication Privacy Laws.

The Electronic Communications Privacy Act (ECPA) imposes penalties against any person who intentionally intercepts an electronic communication with certain exceptions, including in the ordinary course of business. The Stored Communications Act (SCA), part of the ECPA, covers stored electronic communications.

In a case from New Jersey, a restaurant was sued when its managers accessed a private chat group on MySpace that had been created by two employees to disparage the restaurant. The restaurant fired the two employees and they sued, alleging violation of the ECPA. A jury found the restaurant liable because although another employee had provided her log-in information to a manager, she felt coerced into providing the manager her password. Evidence also indicated that the managers accessed the chat group on several occasions and that it was clear on the website that the chat group was intended to be private and accessible only to invited members. Further, the managers continued to access the chat group even after realizing the employee had reservations about having provided her password. *Pietrylo v. Hillstone Restaurant Group*, 2008 WL 6085437 (D.N.J.). Punitive damages were awarded because the violation was found to have been willful and intentional.

4. Freedom of Speech.

When a public employee speaks as a citizen on a matter of public concern, the speech can be entitled to First Amendment protection. This means the employee cannot be disciplined or retaliated against for engaging in the speech. On the other hand, when a public employee speaks as an employee on matters only of personal interest, the employee's speech may not be protected. However, employees never have the right to reveal confidential information or to engage in obscene, harassing, or threatening speech. These considerations should be taken into account prior to disciplining an employee for on-line communications.

5. Protected Union Activity.

State collective bargaining law protects certain types of union activity. Before an employee is disciplined for online behavior, the employer should also verify that the conduct does not constitute protected union activity.

6. Discrimination.

An employee faced with discipline for defaming a co-worker on Facebook or misusing sick leave could accuse the employer of discrimination if other employees engage in similar misconduct without repercussion. It is important, therefore, to be consistent about any monitoring or discipline that occurs. This also highlights the need for managers and HR professionals to exercise discretion in the choice of online "friends." Once a manager becomes aware of their "friend's'" potential work-related misconduct, they must act upon the information or ignore it at their peril. A manager aware of misconduct who chooses to ignore it could later be accused of discrimination when someone else is disciplined for the same behavior.

For example, the Fire Chief of the City of Savannah, Georgia, found out that one of his probationary firefighters had posted unauthorized photographs of the Fire Department next to two photographs of herself, partially undressed, on her MySpace page. The Chief decided to issue an oral reprimand to the employee for bringing discredit to the Department and using her position to enhance and seek personal publicity (the photos were apparently taken in connection with an effort to obtain modeling work). During the meeting to discuss her oral reprimand, the firefighter became hostile and argumentative, and she was subsequently terminated for that behavior.

The firefighter sued the City, the Fire Department, the Mayor, and the Fire Chief, alleging discrimination based on gender, race, and national origin. She claimed other firefighters had similar MySpace pages and she had been singled out. The Eleventh Circuit Court of Appeals decided that even if other firefighters had violated the same rules and regulations, the Fire Chief lacked knowledge of such. The Court wrote, "Absent proof of such knowledge, Marshall cannot establish a *prima facie* case of discrimination." *Marshall v. Mayor and Alderman of the City of Savannah, George, et al*, 2010 WL 537852 (C.A.11 (Ga.)).

This case illustrates the consequences of having knowledge of employees' social media postings.

F. Other Legal Considerations.

1. Public Records Act.

While beyond the scope of this presentation, it is worth mentioning the Pandora's Box that the Public Records Act creates for the use of social media by public employees. State and local records retention and disclosure laws apply to social media content that contains "information relating to the conduct of government or the performance of any

governmental or proprietary function prepared, owned, used, or retained by any state or local agency". RCW 42.56.010(2). Just as a public employee who takes a report home to work on it should expect that the report will be a public record, a public employee who posts a Facebook update from a home computer relating to the conduct of government or the performance of a governmental function may have to treat that content as a public record subject to retention schedules and public disclosure.[2]

G. Minimizing Risks Arising from Social Media Use Through Your Personnel Policies.

Even if some of us might prefer it, we cannot turn back the clock – for better and for worse, social media has entered the workplace and is undoubtedly here to stay. While there is no way to completely avoid the issues and risks arising from this new technology, employers can certainly take steps to reduce and manage those risks through clear personnel policies establishing expectations and prohibitions. An employer might adopt a stand-alone "social media" policy, or it might revise existing policies to incorporate and address social media issues. Either way, employers should consider incorporating the following kinds of provisions into their personnel policies.

1. Address the extent to which personal use of employer internet and related technology is permitted.

Some employers believe that the best way to reduce risk is to prohibit all personal use of employer computers and computer systems (*e.g.*, no internet access for personal reasons, no personal email while at work). Other employers believe such a policy is unrealistic and bad for morale. Ultimately, this is a policy choice for the employer to make. If some personal use is permitted, however, it is advisable to establish some ground rules. At a minimum, a policy should provide that personal use cannot interfere with the employee's work. See, for example, the attached policy permitting and explaining *de minimus* use.

2. Make clear that employees have no expectation of privacy in their use of employer computer and technology systems, and be specific as to what systems are encompassed; advise that monitoring will occur to ensure compliance.

Many employers already have a general statement to the effect that employees should have no expectation of privacy in their computers, desks, etc. Policies should be updated to make clear that this lack of privacy encompasses files and information saved, reviewed or transmitted via all employer technology resources, including computer files, computer

[2] On a related topic, City Council members should be cautious about "friending" each other on social networking sites to avoid unintentionally triggering the requirements of the Open Public Meetings Act.

servers, emails, internet usage, telephones, cellular phones, voicemail, and text messages. In addition to maintaining such a policy, employers must ensure that supervisors do not undermine this policy by assuring employees that personal files and messages will never be reviewed.

3. **Emphasize that an employee's use of technology resources may not violate the employer's policy prohibiting discrimination and harassment or any other work rule.**

   Most employer harassment policies reference the kinds of behavior that have traditionally been found to constitute harassment, such as physical touching, lewd or offensive comments, cartoons and posters, etc. Some policies have been updated to include references to inappropriate email or internet use. Policies should be updated even further to reference the ever-expanding list of ways in which employees can harass each other, thanks to technology. For example, a harassment policy should not only prohibit harassment via email and internet usage, but also through offensive text messages, postings on social media sites such as Facebook and MySpace, Twitter and blogs. Employees should also be advised that these prohibitions apply not only at work, but on their personal time to the extent their activities are directed at co-workers or adversely impact the work environment. These points should also be emphasized in an employer's technology and/or social media policies.

4. **Prohibit the disclosure of confidential information, including medical or other highly personal information, regarding other employees.**

5. **Advise that employees should not use the employer's name, logo, or work-related email address in connection with any personal online communications or activities.**

6. **Prohibit any uses that violate local, state or federal law, including defamation.**

7. **Advise employees that any questions about permissible technology use should be directed to one or more designated management representatives.**

   There is simply no way to cover every possible technology situation in a personnel policy, and employees will have to exercise good judgment. That said, employees should be encouraged to seek guidance if they are unclear whether a particular use is appropriate or not.

8. Prohibit managers from recommending or commenting on a current or former employee via social or professional networking sites absent approval from Human Resources.

As stated above, employers may find themselves facing liability based on an employee's postings or recommendations on social media sites. Information posted on such sites creates the same risks as more traditional kinds of employment references. Employers should ensure that all references – whether by telephone, correspondence, email or the internet – are handled in a way that minimizes risk to the employer.

9. Discourage or prohibit the use of personal social media to conduct official city/county/agency business due to the public records retention and disclosure ramifications.

Public employees are generally mindful of the fact that documents and other records they generate as part of their jobs become public records subject to disclosure. But they may not realize that conferring with colleagues about a work matter via a social media site can also create records subject to public disclosure. A comprehensive guide to public records disclosure is beyond the scope of these materials, but employees should be reminded that even off-duty use of social media may be subject to public disclosure where public business is conducted.

10. Advise that discipline up to and including discharge will result from violations of the policy.

H. Minimizing Risk by Training Employees.

In addition to maintaining policies addressing social media issues, it is a good idea to train employees to think about the kinds of risks and issues that arise from social media use. We tend to think of social media as a form of entertainment – it can be fun, conversational, can lower social barriers and cause us to be more outgoing than we otherwise might be. For these reasons, in addition to promulgating a technology and/or social media policy, employers should remind employees of the following:

- Electronically transmitted information is not permanently deleted. We may think of online activities as conversational, but there are often permanent records of transmissions and postings that may be subject to discovery in litigation and/or to public disclosure.

- The content and tone of work-related electronic communications should adhere to the same standards as a face-to-face conversation. This is a good rule of thumb for employees to keep in mind.

- E-mails and text messages sent from an employee's personal account to a co-worker's personal account, or shared via a social media site, are covered by the employer's anti-harassment and discrimination policies. Employees may assume that such communications are purely personal, but where they impact work relationships or the work environment, they may support a harassment claim. As a result, employers can be liable for failing to address harassing behavior, and therefore have a right to investigate and address this behavior.

- Employees should be cautious about identifying themselves as employees of the agency on the internet, including social networking sites like Facebook. Once they indicate their official title, postings that undermine the employer's reputation could lead to discipline.

- Supervisors and managers should use good judgment in "friending" or otherwise interacting with subordinates on social media sites. A subordinate employee might feel uncomfortable about an invitation from his/her manager to be a Facebook "friend;" the employee may not want to share information on his/her personal page with a manager, and yet might be concerned that declining the invitation could have work repercussions. An employer should not necessarily prohibit these interactions, but should ensure that managers think about these kinds of interactions in the same way they do other forms of socialization with subordinates.

- Supervisors and managers cannot undermine the employer's statements that employees have no expectation of privacy in the information created, transmitted or stored on the employer's systems.

- Employees should not conduct official city business through the use of personal social media. As explained above, such conduct can be subject to public records disclosure and retention requirements.

- Employees should be warned about posting, uploading, or creating any social media content on employer equipment that is known to be false, misleading, or fraudulent. They should also be encouraged not to post photos that infringe on trademark, copyright, or patent rights of others.

- Employees should be counseled that if they would be embarrassed to see their social media posting appear in the news, they should not post it.

APPENDIX

SAMPLE ELECTRONIC COMMUNICATION AND TECHNOLOGY POLICY

The City's objective is to maximize the use of electronic communication and technology as a means of reducing costs and increasing productivity. The City provides communication resources capable of offering email, text messages, internet, telephone and voicemail, fax machines, cell phones, personal digital assistants, and other electronic communications devices (collectively referred to as the City's Technology Resources) to assist and facilitate City business. The primary purpose of the City's Technology Resources is to facilitate the provision of services to the public in a manner consistent with the City's goals and values. De minimus, incidental personal use of the City's Technology Resources is permitted if it conforms to the requirements of this policy. The City expects employees to use their best judgment when using Technology Resources and to consider whether a given use is in the public's best interests.

No Expectation of Privacy. By using the City's Technology Resources, employees understand and agree that they have no expectation of any privacy or confidentiality in any information they create, store, or transmit using these resources. This includes but is not limited to all computer files and information saved, reviewed, or transmitted via all of the City's Technology Resources, including but not limited to computer files, computer servers, emails, internet usage, telephones, cell phones, voicemail, and text messages, and applies to all information created, stored or transmitted during an employee's incidental personal use. No manager or other City employee is authorized to provide assurances that such information is private. Employees' use of the City's Technology Resources can and will be monitored, and any information created, stored, or transmitted using City equipment may be inspected by the City at any time. Employees should also understand that email messages and other forms of electronic information, including documents created on City computers, may be considered public records subject to retention requirements and public disclosure, as well as release in the event of litigation involving the City.

Ownership. All software, programs, applications, templates, data, files, and web pages residing on City computer systems or storage media or developed on City computer systems are the property of the City. The City can access, copy, modify, destroy, and delete this property.

Confidentiality. Confidential and sensitive information may not be removed from the workplace or disclosed without authorization, unless required by law.

Acceptable Uses. The City's Technology Resources are to be used for City business. Incidental, de minimus personal use may be permitted where, in the judgment of the employee's supervisor or department director, such use does not interfere with the employee's or the department's productivity. Generally speaking, incidental, de minimus personal use means: (1) occasional and of short duration; (2) done on an employee's personal time, such as a lunch break; (3) does not interfere with job responsibilities; (4) does not result in any expense to the City; (5) does not solicit or promote commercial ventures; (6) does not utilize excessive network resources; and (7) does not constitute a prohibited use, discussed below. Employees should be mindful that

personal messages and data on the City's system are not private and may be subject to public disclosure.

Prohibited Uses. Use of the City's Technology Resources to engage in any communication that violates federal, state, or local laws or regulations, or any City policy, is strictly prohibited at all times. In addition, the following uses of the City's Technology Resources are inappropriate and are prohibited at all times, unless engaged in as part of official City business (such as a criminal investigation) or required by law (such as a public disclosure request):

- Personal commercial use;
- Accessing, receiving or sending pornographic, sexually explicit, or obscene materials;
- Use in connection with any type of prohibited harassment or discrimination, including the transmission of offensive messages derogatory toward any individual or group because of their sex, race, religion, sexual orientation, national origin, age, disability or other protected status;
- Gambling;
- Use for recreational purposes including online games;
- Use that impacts the performance of the City's network, such as viewing streaming video and sending bulk mail;
- Infringing on the trademark, copyright, or patent rights of others, or violating software licensing agreements;
- Use for political purposes, including partisan campaigning;
- Deliberately propagating any virus, malware, spyware, or other code or file designed to disable or otherwise harm any network or system;
- Disclosing confidential information, including medical or other highly personal information about other employees;
- Using abusive, profane, defamatory, threatening, racist, sexist, or otherwise discourteous language in public or private messages;
- Connecting to the City network or any Technology Resource using someone else's security identification login unless authorized by that person;
- Any personal use, even if incidental, that results in an expense to the City; or
- Use that violates any other City or Department policies, rules, or workplace expectations.

Any questions about whether a use is permitted or not should be directed to a supervisor or IT personnel.

Social Media. Social media is the use of blogs, wikis, social networks, virtual worlds, or any other kind of online social interaction. Employees are advised that City rules and policies apply to social media conduct, including policies regarding statements to the media, anti-discrimination

and harassment, prohibitions on releasing confidential information, and this Electronic Communication and Technology Policy. Off-duty, personal use of social media by employees is not prohibited; however, employees are reminded that City rules and policies apply to social media conduct to the same extent as other off-duty conduct.

The following additional rules also apply to employees' use of social media:

- Social media content that relates to City business may be considered a public record subject to retention and disclosure under the Public Records Act. For that reason, employees are prohibited from using personal social media to conduct City business.

- Employees are prohibited from using their City email address, the City's official logo, or the City's name for personal online communication or activities. Employees may not identify themselves in any manner that suggests or implies they are speaking as a representative for the City.

- Employees should not recommend or discuss any current or former City employees on professional networking sites such as LinkedIn without approval from the Human Resources Department.

- Employees may not post, upload, or create any social media content at work or using employer equipment that is known to be false, misleading, or fraudulent.

Violations. Employees who violate this policy are subject to disciplinary action, up to and including termination.