



County Commissioners Association of Ohio

Samples of Social Media, Cell Phone, Computer Use, Etc. Policies

May 13, 2015

PRESENTED BY: JONATHAN J. DOWNES

OSBA Certified Specialist in
Labor and Employment Law
Phone: 614-224-4411
Cell: 614-565-2075
jjd@zrlaw.com

This material is intended solely for informational and presentation purposes only and in no way should be construed as offering or providing legal advice.



**Contact Information:
Jonathan J. Downes**

jjd@zrlaw.com
614.224.4411
614.565.2075 Cell

About Jonathan Downes:

Jonathan Downes brings more than thirty years of experience and expertise in representing public and private employers in all aspects of labor and employment law and human resource management. In addition to negotiating over 500 labor contracts, Jonathan has represented employers in arbitrations, organizing campaigns, and administrative hearings including the State Employment Relations Board. Jonathan has also defended employers in state trial and appellate courts, the Ohio Supreme Court, federal district courts and the United States Court of Appeals for the Sixth Circuit.

When not in negotiations, at court, or teaching a seminar, Jonathan edits Westlaw's Ohio Civil Service and Collective Bargaining Laws Annotated publication. He also edits annually Civil Service Law in Ohio (Westlaw) and contributes to numerous association and trade group publications.

Jonathan is certified by the Ohio State Bar Association as a Specialist in Labor and Employment Law, is AV-Preeminent rated by Martindale Hubbell and selected by peers for "Best Lawyers in America" in the practice areas of "Employment Law – Management" and "Labor Law – Management."® While recognized many times over as a subject-matter expert, Jonathan was selected as one of the Top 50 Central Ohio Lawyers of 2015 and every year since 2004 has been named an Ohio "Super Lawyer."

About Zashin and Rich:

Zashin & Rich Co., L.P.A. ("Z&R") specializes in labor and employment law with offices in Cleveland and Columbus, representing both private and public employers. Members of Z&R have diverse backgrounds and experience which provides depth and understanding of the needs of its clients.

Z&R represents its clients with broad experience in labor negotiations, human resources matters, and civil service. Attorneys of Z&R have collectively negotiated over 1000 contracts and have represented private and public employers in numerous arbitrations, impasse proceedings and in litigation. Attorneys have extensive experience representing private employers, universities and colleges, state agencies, special districts, cities, counties, townships, housing authorities, hospitals and others. Attorneys handle matters at arbitrations, the National Labor Relations Board, the State Employment Relations Board as well as the State Personnel Board of Review, and local civil service commissions.

Z&R representation includes all federal and state discrimination laws, administrative and court proceedings, employee handbooks and manuals, contract administration, strike situations, grievances and arbitration, discipline matters, public pension systems and workers' compensation. Attorneys in the firm have extensive knowledge and experience, both in litigation and providing advice, with various federal laws including FMLA, FLSA, ADA and Title VII Civil Rights. The firm has an extensive insurance defense practice representing several national insurance companies including Chubb, Travelers, and AIG among others. The firm represents clients before the EEOC, OCRC and in state and federal courts in all parts of Ohio.

The firm's Labor & Employment Group has received First Tier ranking in Employment Law-Management in the Cleveland Region and Labor Law-Management in both the Cleveland and Columbus Regions by U.S. News Best Lawyers® "Best Law Firms" in 2014 and 2015.



Samples of Social Media Policies, Cell Phone, Computer Use, Etc. Policies - May 13, 2015

I. SOCIAL MEDIA – EXAMPLE POLICY

A. Purpose

The purpose behind this policy is to make an employee aware of his or her privacy rights and prohibited conduct with respect to an employee's actions and its impact on the Employer when using social media sites on and off duty. This policy is also intended to ensure efficient use of employee time and to minimize any distraction from an employee's assigned tasks and duties. It will allow the Employer to ensure that Employer rules are followed and all employees are treated fair and consistent. Employees shall remember they are paid by public funds and the public holds them to a high standard of professionalism. The Employer has an overriding interest and expectation in deciding what is "spoken" on behalf of the Employer. This policy is not meant to infringe on one's right to free speech, rights under R.C. 4117, or any other protected activity.

B. All employees will be subject to and held accountable for any conduct outlined in Social Media Policy. This policy works in conjunction with other related personnel policies and procedures (e.g. harassment).

C. Social Media refers to the use of websites such as, but not limited to, Facebook, Myspace, Twitter, Flickr, LinkedIn, Instagram. For purposes of this policy, Blogs and other internet forums of shall also be covered. Nothing in this policy is meant to prohibit access to any social media website or Blog which may be work-related.

D. Conduct

1. On Duty Conduct – While at work, an employee may only access social media websites, Blogs and/or other internet forums of communication during their lunch or breaks. This includes access from a personal cellular device (E.g., Blackberry device, Smartphone, iPhone, etc.) during an employee's compensated hours of work.
2. On and Off Duty Conduct – An employee enjoys no expectation of privacy to information posted into cyberspace even while off duty. This includes anything posted to a social media website, Blog, or other similar internet forum of communication. Although information may be posted to a "private" webpage, the employee should be aware this information can still be accessed by the public and other sources in a number of ways. Because of this, an employee needs to use "common-sense" when posting comments, photos, opinions, or any other information related to his or her employment. Any social media activity which portrays the Employer in a negative light will be evaluated and may result in



Samples of Social Media Policies, Cell Phone, Computer Use, Etc. Policies - May 13, 2015

disciplinary action up to and including termination.

3. Prohibited Conduct includes, but is not limited to:
 - a. Posting one's photograph while wearing the Employer's uniform (or other similar attire, which could be misidentified as the official uniform);
 - b. Posting pictures, videos, or comments that are insubordinate with respect to the employee's employment
 - c. Posting pictures, videos, or comments that constitute or could be construed as unlawful behavior;
 - d. Knowingly or recklessly posting false information about the Employer, supervisors, coworkers, public officials, or those who have a relationship with the Employer. This also includes disparagement of a fictitious character or computer-generated likeness that resembles the above.
 - e. Posting, transmitting, or disseminating any pictures or videos of official training, activities, work-related assignments, or statements about or naming clients without the express permission of a supervisor.
 - f. Posting pictures, videos, or comments that are sexual, obscene, violent, offensive, harassing, or pornographic in nature along with any reference to the Employer or individual's employment
4. Employees shall not imply they are speaking on behalf of the Employer unless authorized to do so. Should an employee speak on matters of employment, the employee shall include a disclaimer.
5. Confidential Information – An employee shall not disclose any work-related confidential or proprietary information on any social media website, Blog, or other internet forum of communication. This can include information that may eventually be obtained through a valid public record's request.
6. Employees are encouraged to follow the internal complaint procedure and not take to the internet to voice work-related complaints.
7. Employees found to have violated any part of this policy may be subject to discipline up to and including termination.



Samples of Social Media Policies, Cell Phone, Computer Use, Etc. Policies - May 13, 2015

8. Any deviation from the above policy shall be approved by the Employer in writing.
9. Any questions regarding the policy should be directed to the employee's immediate supervisor.
10. Employees shall take note of the following: DELETE DOES NOT MEAN DELETE. Once something is posted into cyberspace it remains there.

II. ELECTRONIC DEVICES, COMPUTER, ETC. EXAMPLE POLICY

Computer and Technology Use, Internet, Emails, Social Media, Cell Phones Information Technology Policy

Employees ("users") are provided with Internet access and electronic communications services (which may include, but are not limited to, computers, e-mail, cell phones, iPhones, iPads, PDAs, personal computers and the like) as required for the performance and fulfillment of job responsibilities. All users are obligated to make effective, safe and responsible use of this technology. This policy applies to all employees, including regular full-time, permanent part-time, temporary, and seasonal employees who are provided access to the technology systems.

The Township offers this access to technology for the purpose of increasing productivity and not for non-work related activities. Specifically, this technology is meant to enhance operations by enabling users to, among other things: locate and retrieve information; communicate more effectively with other departments, employees, and organizations; and more easily publish information of interest to the community and the general public. Users must understand that any connection to the Internet offers an opportunity for non-authorized users to view or access information stored in the system. Therefore, it is important that all connections be secured, controlled and monitored.

Electronic equipment and communications systems provided are considered to be Township property to be used for valid business purposes only. All communications and/or information created, stored, received, sent or otherwise transmitted on or through provided technology, including without limitation the Internet, intranet, email, servers, personal computers, iPads, associated hardware and software, online services and other electronic communications services, are considered Township property.

There shall be no expected right of privacy for any matter related to using equipment provided, including no personal privacy right in any matter passing through, viewed,



Samples of Social Media Policies, Cell Phone, Computer Use, Etc. Policies - May 13, 2015

downloaded, printed, created, stored, received, sent or otherwise transmitted from Township provided technology and equipment. All users should understand that the Township reserves and intends to exercise the right to monitor, review, intercept, access and disclose all Internet usage, email communications sent or received, and all cell phone, iPhone, iPad and PDA usage, if necessary, to ensure that the system is being used for business purposes in compliance with this policy, to ensure that all other policies (including without limitation those related to harassment and discrimination) are being followed, and to be able to access information in an employee's email or other electronic communications system in the event that the employee is unavailable to do so. Electronic audits of Internet activity and other electronic communications by Township users will be implemented to identify and properly deal with unauthorized activity.

Internet Access, Email, etc.

Restrictions may apply to access, of all users, to certain unapproved Internet sites and capabilities (ex: YouTube and instant messenger capabilities).

Permitted Use

The Internet and electronic communications services are intended for the purposes of conducting Township business. Valid business purposes include, but are not limited to:

- Locating, retrieving, collecting and/or disseminating information in connection with business;
- Communicating with other departments and employees, as well as with outside contractors, businesses, individuals or organizations currently or potentially doing business with or assisting with the business of the Township;
- Conducting research to obtain information and material related to Township issues;

Prohibited Use

Internet and electronic communications services should not be used for any prohibited purpose. Prohibited usage may result in the cancellation or loss of privileges, Prohibited usage includes, but is not limited to:

- Conducting personal business activities or seeking personal financial gain;
- Playing games during working hours;



Samples of Social Media Policies, Cell Phone, Computer Use, Etc. Policies - May 13, 2015

- Bringing actual or potential embarrassment or harm to the Township;
- Conducting illegal activities or otherwise violating federal, state, or local laws;
- Receiving, transmitting, downloading, viewing, or printing offensive materials of any kind, including any obscene or pornographic materials;
- Receiving, transmitting, downloading, viewing, or printing any materials of a derogatory, inflammatory, discriminatory, harassing, violent or threatening in nature, including any content regarding an individual's or group's race, national origin, gender, age, marital status, sexual orientation, religion or disability;
- Downloading and/or installing software, games or any files or programs which could potentially change system configuration without the consent of authorized Information Technology personnel;
- Removing and/or copying software, shared files or programs without the consent of authorized Information Technology personnel;
- Distributing or printing copyrighted materials, which include articles, software or intellectual property, in violation of the copyright laws;
- Copying programs from Township owned systems for personal use;
- Spamming email accounts or forwarding chain letters;
- Disclosing confidential information or otherwise violating the privacy rights of the Township or its employees, citizens or business associates;
- Using the Internet or electronic communications systems of another employee without authorization;
- Vandalizing data of another user, including uploading or creating of computer viruses; and/or
- Purchasing goods, materials, or services via the Internet using a Township credit card or other credit means without having proper authorization.

User Responsibilities

- Ensuring the security of their accounts and related passwords. Passwords should never be shared between users or be in plain sight. If the integrity of a password has been compromised, it should be changed and/or Supervisors should be notified.
- Abiding by existing federal, state and local telecommunications and networking laws and regulations;



Samples of Social Media Policies, Cell Phone, Computer Use, Etc. Policies - May 13, 2015

- Minimizing unnecessary network traffic that may interfere with the ability of others to make effective use of Township network resources and to conduct normal business activities;
- Avoiding the overload of networks with excessive data, or wasting other Township technical resources;
- Exercising good judgment and generally accepted rules of network etiquette when using the Internet or other electronic communications services to avoid offense to others;
- Maintaining the integrity and confidentiality of all Township information;
- Exercising good judgment when providing information to other individuals and using all reasonable safeguards to avoid the mistaken distribution of another's information. The transmission of confidential, sensitive or personal information shall only be in accord with current procedures and regulations. Employees should disclose such information or messages from the electronic communications system only to authorized individuals with a need to know.

Violations

If it is determined that a user has violated any of the above policy guidelines, the user will be considered to have misused Township property and will be subject to disciplinary action, up to and including termination, as well as the loss of electronic communications privileges. If necessary, the Township will advise appropriate legal authorities of any illegal activities.

Email

This policy provides the employees with effective, consistent standards in regards to the use of the electronic mail systems (email). This policy applies to all the employees at all facilities. Violations of any guidelines listed above may result in disciplinary action up to and including termination. If necessary appropriate legal officials will be advised of any illegal violations.

Employee Responsibilities

All electronic communications and stored information transmitted, received, or archived in the Township's information system are the property of the Township. The Township reserves the right to access and disclose all messages sent by email. Employees should have no expectation of privacy with respect to any email coming into or going out of Township resources, particularly those which come into, or go out of, a Township email account. Township email



Samples of Social Media Policies, Cell Phone, Computer Use, Etc. Policies - May 13, 2015

accounts are provided in order to carry out communications for Township or Township-related business only. Employees may not access their personal email accounts through the computer system.

Social Media

There are many tools available today that enable people to publish and share content on the public Internet. These include social media and networking sites such as Facebook, Twitter, Yelp, YouTube, and foursquare, subscription services such as Angie's List, as well as blogs, blog comments, forum posts, wikis, and other similar sites.

Employees are free to participate in any of these forms of communication with their personally-owned devices during their personal non-work time. The Township respects the right of its employees to use social media sites and other parts of the public Internet as a medium of self-expression, communication, and public conversation. The Township does not discriminate against employees who use these media for personal interests and affiliations or for other lawful purposes.

However, employees should keep in mind that their postings can affect how the general public perceives the Township. The Township has the right to make sure that nobody has made unauthorized use of or discloses confidential information (e.g., personal and protected information about employees and/or citizens). Employees are cautioned that they should have no expectation of privacy while using the public Internet, even on their own personal time, and even when using their own personal equipment. Employees' public postings on social media and other Internet sites can be viewed by anyone, including the Township's management.

The following guidelines apply to all use of social media or the public Internet by Township employees, even when on their own personal time and on their own personal equipment:

- Employees are free to identify themselves as a Township employee if they wish. However, they should state that their views are their own, and do not reflect those of the Township administration.
- Employees are free to express themselves as private citizens on social media sites to the degree that their speech does not impair working relationships of the Township for which loyalty and confidentiality are important, impede the performance of duties, impair discipline and harmony among coworkers, or negatively affect the public perception of the Township.



Samples of Social Media Policies, Cell Phone, Computer Use, Etc. Policies - May 13, 2015

- As public employees, Township employees are cautioned that speech on-or-off-duty, made pursuant to their official duties-that is, that owes its existence to the employee's professional duties and responsibilities-is not protected speech under the First Amendment and may form the basis for discipline if deemed detrimental to the Department. Township employees should assume that their speech and related activity on social media sites will reflect upon their office and this Township.
- Township employees shall not post, transmit, or otherwise disseminate any information to which they have access as a result of their employment without written permission from the Trustees.
- For safety and security reasons, Township employees are cautioned not to disclose their employment with Township nor shall they post information pertaining to any other member of the Township without their permission. As such, personnel are cautioned not to do the following:
 - Display Township department logos, uniforms, or similar identifying items on personal web pages.
 - Post personal photographs or provide similar means of personal recognition that may cause them to be identified as an employee of the Township. Police Officers who are, or who may reasonably be expected to work in undercover operations, shall not post any form of visual or personal identification.
 - If an employee is contacted by anyone about one of their posts, including a commenter or a member of the press, and is asked to discuss confidential Township information, the employee must speak with his or her supervisor before responding.
 - Only employees who are specifically authorized by the Township are permitted to prepare and modify content for the Township's website, any official Township blogs, and any of the Township's official social media presences. If an employee is uncertain about whether or not he or she is permitted to post certain content, he or she must discuss the proposed content with his or her supervisor prior to posting.
 - If an employee sees a posting on the Internet from a member of the public that speaks adversely about any Township operation or service, they should forward the post to their supervisor instead of responding directly to the poster.
 - Employees may not claim to speak on behalf of the Township in an official capacity on the public Internet or in any social networking service unless they have been



Samples of Social Media Policies, Cell Phone, Computer Use, Etc. Policies - May 13, 2015

specifically authorized to do so.

- Employees may not discuss or disclose on the public Internet or in any social networking service any confidential or other information they obtained through their employment with the Township. All public requests for information must be submitted through the records request policy.
- Employees may not post or view any content on social media sites or to the public Internet during working time, except as part of the employee's official assigned job duties.
- Employees may not post any threats of violence or any unlawfully harassing or discriminatory content about any of their co-workers, or any person.
- Any employee found to be violating this Policy is subject to disciplinary action, including discharge.

Cell Phone Policy Cellular Phone, Electronic Device

This policy outlines the use of personal cell phones/electronic devices at work, the personal use of Township cell phones/electronic devices and the safe use of cell phones/electronic devices by employees while driving.

Personal Cellular Phones/Electronic Devices

While at work employees are expected to exercise the same discretion in using personal cellular phones/electronic devices as is expected for the use of Township phones or devices. Excessive personal calls/electronic device use during the work day, regardless of the phone/device used, interfere with employee productivity and distract others. Employees must limit personal calls and electronic device use to non-working time (i.e., authorized breaks and lunch periods), not be used while driving Township vehicles or using Township equipment, and ensure that friends and family members are aware of the Township's policy. Flexibility will be provided in circumstances demanding immediate attention or for emergencies. Use which is beyond minimal needed use will be subject to discipline.

Where an employee's duties require immediate access to an employee the Township may issue a pager, cellular phone or a hand-held radio (i.e., a "walkie-talkie") to an employee for work-related communications.

*Samples of Social Media Policies, Cell Phone, Computer Use, Etc. Policies - May 13, 2015*

Employees in possession of Township equipment are expected to protect the equipment from loss, damage or theft. Upon resignation or termination of employment, or any time upon request, the employee may be asked to produce the equipment for return or inspection. Employees unable to present the equipment in good working condition within the time period requested (i.e. 24 hours) may be expected to bear the cost of a replacement.

Safety Issues for Cellular Phone/Electronic Device Use

Employees whose job responsibilities include regular or occasional driving and who are issued a cell phone/electronic device for business use are expected to refrain from using their phone/device while driving. Safety must come before all other concerns. Regardless of the circumstances, including slow or stopped traffic, employees are strongly encouraged to pull off to the side of the road and safely stop the vehicle before placing or accepting a call or using an electronic device. If acceptance of a call or use of the device is unavoidable and pulling over is not an option, employees are expected to keep the call/use short, use hands- free options if available, refrain from complicated or emotional discussions and keep their eyes on the road. Special care should be taken in situations where there is traffic, inclement weather or the employee is driving in an unfamiliar area.

Employees whose job responsibilities do not specifically include driving as an essential function, but who are issued a cell phone/electronic device for uses related to their employment with the Township are also expected to abide by the provisions above. Under no circumstances are employees allowed to place themselves or others at risk to fulfill work needs. Employees who are charged with traffic violations resulting from the use of their phone/electronic device while driving will be solely responsible for all liabilities that result from such actions. Violations of this policy will be subject to discipline up to and including termination.

III. GENERAL COMPUTER USE POLICIES - EXAMPLE POLICY**1. Computer and Technology Use, Cell Phones****1.1. Information Technology Policy**

Employees are provided with Internet access and electronic communications services (which may include, but are not limited to, computers, e-mail, cell phones, iPhones, iPads, PDAs, personal computers and the like) as required for the performance and fulfillment of job responsibilities. All employees are obligated to make effective, safe and responsible use of this technology. This policy applies to all employees, including regular full-time, permanent part-time, temporary, and seasonal employees who are provided access to the technology systems.



Samples of Social Media Policies, Cell Phone, Computer Use, Etc. Policies - May 13, 2015

The City offers this access to technology for the purpose of increasing productivity and not for non-work related activities. Specifically, this technology is meant to enhance operations by enabling users to, among other things: locate and retrieve information; communicate more effectively with other departments, employees, and organizations; and more easily publish information of interest to the community and the general public. Users must understand that any connection to the Internet offers an opportunity for non-authorized users to view or access information stored in the system. Therefore, it is important that all connections be secured, controlled and monitored.

Electronic equipment and communications systems provided are considered to be City property to be used for valid business purposes only. All communications and/or information created, stored, received, sent or otherwise transmitted on or through provided technology, including without limitation the Internet, intranet, email, servers, personal computers, iPads, associated hardware and software, online services and other electronic communications services, are considered City property.

There shall be no expected right of privacy for any matter related to using equipment provided, including no personal privacy right in any matter passing through, viewed, downloaded, printed, created, stored, received, sent or otherwise transmitted from City-provided technology and equipment. All employees should understand that the City reserves and intends to exercise the right to monitor, review, intercept, access and disclose all Internet usage, email communications sent or received, and all cell phone, iPhone, iPad and PDA usage, if necessary, to ensure that the system is being used for business purposes in compliance with this policy, to ensure that all other policies (including without limitation for instance those related to harassment and discrimination) are being followed, and to be able to access information in an employee's email or other electronic communications system in the event that the employee is unavailable to do so. Electronic audits of Internet activity and other electronic communications by City employees may be implemented to identify and properly deal with unauthorized activity.

1.2. Internet Access, Email, Public Records etc.

Restrictions may apply to access, of all users, to certain unapproved Internet sites and capabilities (ex: YouTube and instant messenger capabilities).

Emails are public records under State Law and are subject to public records requests. Emails must be maintained and may be deleted only according to the public records policy.



Samples of Social Media Policies, Cell Phone, Computer Use, Etc. Policies - May 13, 2015

Permitted Use

The Internet and electronic communications services are intended for the purposes of conducting City business. Valid business purposes include, but are not limited to:

- Locating, retrieving, collecting and/or disseminating information in connection with business;
- Communicating with other departments and employees, as well as with outside contractors, businesses, individuals or organizations currently or potentially doing business with or assisting with the business of the City;
- Conducting research to obtain information and material related to City issues; and
- Limited personal use that does not result in the disruption of network operation or interfere with personal productivity at work. Personal use of City technology and electronic devices must be kept to the minimum amount of time needed to address a situation. Excessive use will be determined on a case-by-case basis.

Prohibited Use

Internet and electronic communications services should not be used for any prohibited purpose. Prohibited usage may result in the cancellation or loss of privileges. Any non-work related use is defined as a prohibited use. Prohibited usage includes, but is not limited to:

- Conducting personal business activities or seeking personal financial gain.
- Playing games during working hours.
- Bringing actual or potential embarrassment or harm to the City.
- Conducting illegal activities or otherwise violating federal, state, or local laws.
- Receiving, transmitting, downloading, viewing, or printing offensive materials of any kind, including any obscene or pornographic materials.
- Receiving, transmitting, downloading, viewing, or printing any materials of a derogatory, inflammatory, discriminatory, harassing, sexually explicit, obscene, offensive, defamatory, violent or threatening in nature, or other material which is inappropriate, including any content regarding an individual's or group's race,



Samples of Social Media Policies, Cell Phone, Computer Use, Etc. Policies - May 13, 2015

national origin, gender, age, marital status, sexual orientation, religion or disability.

- Downloading and/or installing software, games or any files or programs which could potentially change system configuration without the consent of authorized Information Technology personnel.
- Removing and/or copying software, shared files or programs without the consent of authorized Information Technology personnel.
- Any social media use that is unrelated to an employee's duties and responsibilities.
- Use of any streaming or websites that impair system operations.
- Downloading, distributing or printing copyrighted materials, which include articles, software or intellectual property, in violation of the copyright laws.
- Copying programs from City owned systems for personal use or non-City use.
- Spamming email accounts or forwarding chain letters.
- Disclosing confidential information or otherwise violating the privacy rights of the City or its employees, citizens or business associates.
- Using the Internet or electronic communications systems of another employee without authorization.
- Vandalizing data of another user, including uploading or creating of computer viruses.
- Purchasing goods, materials, or services via the Internet using a City credit card or other credit means without having proper authorization.
- Violating any state or federal law.
- Other uses as determined by the City.



Samples of Social Media Policies, Cell Phone, Computer Use, Etc. Policies - May 13, 2015

1.3. User, Employee Responsibilities

User Responsibilities

- Ensuring the security of their accounts and related passwords. Passwords should never be shared between users or be in plain sight. If the integrity of a password has been compromised, it should be changed and/or the Information Technology personnel or Department should be notified.
- Abiding by existing federal, state and local telecommunications and networking laws and regulations;
- Minimizing unnecessary network traffic that may interfere with the ability of others to make effective use of City network resources and to conduct normal business activities;
- Avoiding the overload of networks with excessive data, or wasting other City technical resources;
- Exercising good judgment and generally accepted rules of network etiquette when using the Internet or other electronic communications services to avoid offense to others;
- Maintaining the integrity and confidentiality of all City information;
- Exercising good judgment when providing information to other individuals and using all reasonable safeguards to avoid the mistaken distribution of another's information. The transmission of confidential, sensitive or personal information shall only be in accord with must follow current procedures and regulations. Employees should disclose such information or messages from the electronic communications system only to authorized individuals with a need to know.
- All dissemination of public records must follow the rules in this handbook and all public records policies and laws.
- Access personal email accounts.



1.4. Violations

If it is determined that a user has violated any of the above policy guidelines, the user will be considered to have misused City property and will be subject to disciplinary action, up to and including termination, as well as the loss of electronic communications privileges. If an employee belongs to a union, any violation by the employee will be subject to the disciplinary process of the applicable collective bargaining agreement. If necessary, the City will advise appropriate legal authorities of any illegal activities.

1.5. Email Use Policy

This policy provides the employees with effective, consistent standards in regards to the use of the electronic mail systems (email). This policy applies to all employees. Violations of any guidelines listed above may result in disciplinary action up to and including termination. If necessary appropriate legal officials will be advised of any illegal activities.

All electronic communications and stored information transmitted, received, or archived in the City's information system are the property of the City. The City reserves the right to access and disclose all messages sent by email. Employees should have no expectation of privacy with respect to any email coming into or going out of City resources, particularly those which come into, or go out of, a City email account. City email accounts are provided in order to carry out communications for City or City-related business only. Employees may not access their personal email accounts through the computer system.

1.6. Social Media

Public employees have responsibilities, higher standard of conduct, and image in the public to follow and maintain.

There are many tools available today that enable people to publish and share content on the public Internet. These include social media and networking sites such as Facebook, Twitter, Yelp, YouTube, and foursquare, subscription services such as Angie's List, as well as blogs, blog comments, forum posts, wikis, and other similar sites.

Employees are free to/may participate in any of these forms of communication using personal equipment during their personal non-work time. The City respects the right of its employees to use social media sites and other parts of the public Internet as a medium of self-expression,



Samples of Social Media Policies, Cell Phone, Computer Use, Etc. Policies - May 13, 2015

communication, and public conversation. The City does not discriminate against employees who use these media for personal interests and affiliations or for other lawful purposes.

However, employees should keep in mind that their postings can affect how the general public perceives the City. The City has the right to make sure that nobody has made unauthorized use of or discloses confidential information (e.g., personal and protected information about employees and/or citizens). Employees are cautioned that they should have no expectation of privacy while using the public Internet, even on their own personal time, and even when using their own personal equipment. Employees' public postings on social media and other Internet sites can be viewed by anyone, including the City's management.

The following guidelines apply to all use of social media or the public Internet by Company employees, even when on their own personal time and on their own personal equipment:

- Employees are free to identify themselves as a City employee if they wish. (Certain law enforcement positions may be exempt.) However, they should state that their views are their own, and do not reflect those of the City administration.
- If an employee is contacted by anyone about one of their posts, including a commenter or a member of the press, and is asked to discuss confidential City information, the employee must speak with his or her supervisor before responding.
- Only employees who are specifically authorized by the City are permitted to prepare and modify content for the City's website, any official City blogs, and any of the City's official social media sites. If an employee is uncertain about whether or not he or she is permitted to post certain content, he or she must discuss the proposed content with his or her supervisor prior to posting.
- If an employee sees a posting on the Internet from a member of the public that speaks adversely about any City operation or service, they should forward the post to their supervisor instead of responding directly to the poster.
- Employees may not claim to speak on behalf of the City in an official capacity on the public Internet or in any social networking service unless they have been specifically authorized to do so.



Samples of Social Media Policies, Cell Phone, Computer Use, Etc. Policies - May 13, 2015

- Employees may not discuss or disclose on the public Internet or in any social networking service any confidential information they obtained through their employment with the City.
- Employees may not post or view any content on social media sites or to the public Internet during working time, except as part of the employee's official assigned job duties.
- Employees may not post any threats of violence or any unlawfully harassing or discriminatory content about any of their co-workers, or any person.
- Any employee found to be violating this Policy is subject to immediate disciplinary action, including discharge.

1.7. Cellular Phone, Electronic Device

This policy outlines the use of personal cell phones/electronic devices at work, the personal use of City cell phones/electronic devices and the safe use of cell phones/electronic devices by employees while driving.

Personal Cellular Phones/Electronic Devices

While at work employees are expected to exercise the same discretion in using personal cellular phones/electronic devices as is expected for the use of City phones. Excessive personal calls/electronic device use during the work day, regardless of the phone/device used, interfere with employee productivity and distract others. Employees must limit personal calls and electronic device use to non-working time (i.e., authorized breaks and lunch periods) and ensure that friends and family members are aware of the City's policy. Flexibility will be provided in circumstances demanding immediate attention or for emergencies.

Where an employee's duties require immediate access to an employee the City may issue a pager, cellular phone or a hand-held radio (i.e., a "walkie-talkie") to an employee for work-related communications.

Employees in possession of City equipment are expected to protect the equipment from loss, damage or theft. Upon resignation or termination of employment, or any time upon request, the employee may be asked to produce the equipment for return or inspection. Employees unable to



Samples of Social Media Policies, Cell Phone, Computer Use, Etc. Policies - May 13, 2015

present the equipment in good working condition within the time period requested (i.e. 24 hours) may be expected to bear the cost of a replacement.

Safety Issues for Cellular Phone/Electronic Device Use

Employees whose job responsibilities include regular or occasional driving and who are issued a cell phone/electronic device for business use are expected to refrain from using their phone/device while driving. Safety must come before all other concerns. Regardless of the circumstances, including slow or stopped traffic, employees are strongly encouraged to pull off to the side of the road and safely stop the vehicle before placing or accepting a call or using an electronic device. If acceptance of a call or use of the device is unavoidable and pulling over is not an option, employees are expected to keep the call/use short, use hands-free options if available, refrain from complicated or emotional discussions and keep their eyes on the road. Special care should be taken in situations where there is traffic, inclement weather or the employee is driving in an unfamiliar area.

Employees whose job responsibilities do not specifically include driving as an essential function, but who are issued a cell phone/electronic device for uses related to their employment with the City are also expected to abide by the provisions above. Under no circumstances are employees allowed to place themselves or others at risk to fulfill work needs. Employees who are charged with traffic violations resulting from the use of their phone/electronic device while driving will be solely responsible for all liabilities that result from such actions. Violations of this policy will be subject to discipline up to and including termination.