7.9 Computer Conduct, Information, Security and Social Networking

Purpose: To state the City's policies regarding the use of all Communication Media, which include, but are not limited to the City's phones, cell phones, computers, access to the Internet and the City's intranets, email, fax and voicemail; to ensure that all City employees, interns and volunteers are aware of their responsibility to protect the security and integrity of vital information; to define for City employees, interns and volunteers the guidelines for participation in social media, which includes, but is not limited to blogs, forums, and social networking sites such as Twitter, Facebook, LinkedIn, YouTube and MySpace.

Policy: **The City respects the individual privacy of its employees. However, the City's Communication Media are the property of the City and, as such, are to be used for legitimate business purposes only. All email, voicemail and Internet messages are public records subject to possible disclosure to the public pursuant to the provisions of the Open Public Records Act.**

All data is the property of the City of Ocean City. Employees, interns and volunteers may access only data for which a Data Manager has given permission. All employees must take appropriate actions to ensure that City data is protected from unauthorized access, use or distribution consistent with these policies.

The City encourages employees to share information with co-workers and with those outside the City for the purpose of gathering information, generating new ideas and learning from the work of others. Social media provide inexpensive, informal and timely ways to participate in an exchange of ideas and information. However, information posted on a website is available to the public; therefore, employees must adhere to the following guidelines for their participation in social media.

Scope: These policies apply to all employees, interns and volunteers of the City of Ocean City. To the extent feasible, these policies shall also apply to consultant service providers and external auditors who perform work for the City.

Definitions:

Data: Electronically-stored files, programs, tables, data bases, audio and video objects, spreadsheets, reports and printed or microfiche materials which serve a City business purpose, regardless of who creates, processes or maintains the data, or whether the data is processed manually or though any of the City's mainframe, midrange or workstations; servers, routers, gateways, bridges, hubs, switches and other hardware components of the City's local or wide-area networks.

Definitions (continued):

Data Manager: An employee with responsibility to control and supervise the use of specific data; permit access to data users; and delegate responsibilities. The IT Division is responsible for specifying data security requirements and custodial requirements to data users.

Data User: An employee, intern or volunteer who has received permission from a Data Manager to access and use the City's data. Data users must comply with data security standards, guidelines, practices and procedures developed by the City.

Security Administrator: A designated employee from the IT Division who is responsible for implementing data security policies, practices and procedures, and for maintaining the City's entire infrastructure security environment.

Procedures:

The City's Communication Media may not be used to solicit for commercial ventures, religious or political causes, outside organizations, or other non-job-related causes. The City's Communications Media may not be used to communicate improper messages that are, or that the recipient may find to be, disruptive, offensive or harmful.

Employees may not access a file or retrieve and store information other than where authorized. In addition, the City's Communication Media may not be used for the downloading, transmitting or possessing of messages or pictures, which are derogatory, defamatory, pornographic or sexually explicit.

Employee communications transmitted by the City's Communication Media are not private to the individual. **All Communication Media and all communications and stored information transmitted, received, or contained in or through such media may be monitored by the City. The City reserves the absolute right to access, review, audit and disclose all matters entered into, sent over, placed in storage in the City's Communication Media.**

City personnel may monitor the City's Communication Media to ensure the City's legitimate business interest in the proper utilization and protection of its property. Monitoring may also be used to ensure that the City's Anti-General Harassment Policy (2.29) and Anti-Sexual Harassment Policy (2.30) are being followed, and that any applicable data is being protected from inappropriate use or disclosure.

Procedures (continued):

By using the City's equipment and/or Communication Media, employees consent to have such use monitored at any time, with or without notice, by City personnel. The existence of passwords does not restrict or eliminate the City's ability or right to access electronic communications. Personal accounts and related information should not be accessed or stored on City equipment and/or communication media. The City cannot require an employee to provide the password to his/her personal account.

All email, voicemail and Internet messages (including any technology-based messaging) are official documents subject to the provisions of the Open Public Records Act (NJSA 47:1A-1). Employees of the City of Ocean City are required to use the assigned municipal email account for ALL City business and correspondence. The use of private email accounts for ANY City business or during business hours is strictly prohibited.

Employees must not reveal or publicize confidential City information. Confidential proprietary or sensitive information may be disseminated only to individuals with a need and a right to know, and where there is sufficient assurance that appropriate security of such information will be maintained. Such information includes, but is not limited to the transmittal of personnel information such as medical records or related information. In law enforcement operations, confidential, proprietary or sensitive information also includes criminal history information, confidential informant identification, and intelligence and tactical operations files.

Any use of the City's name, logos, service marks or trademarks outside the course of the employee's employment, without the express consent of the City, is strictly prohibited.

Except in emergency situations or as part of their officially assigned or regular or permitted duties, employees, interns and volunteers are prohibited from releasing or disclosing any photographs, pictures, digital images of any crime scenes, traffic crashes, arrestees, detainees, people or job-related incident or occurrence taken with a personal or agency analog or digital device, camera or cell phone to any person, entity, business or media or Internet outlet without the prior express written permission of their Department Head or the Business Administrator. (For purposes of this section, an "emergency situation" involves a sudden and unforeseen combination of circumstances or the resulting state that calls for immediate action, assistance or relief, and may include accidents, crimes and flights from accidents or crimes.)

Procedures (continued):

No media advertisement, electronic bulletin board posting, or any other posting accessible via the Internet about the City or on behalf of the City, whether through the use of the City's Communication Media or otherwise, may be issued unless it has first been approved by the Department Head of the City. Under no circumstances may information of a confidential, sensitive or otherwise proprietary nature be placed or posted on the Internet or otherwise disclosed to anyone outside the City.

Because (authorized) postings placed on the Internet through use of the City's Communication Media will display on the City's return address, any information posted on the Internet must reflect and adhere to all of the City's standards and policies.

All users are personally accountable for messages that they originate or forward using the City's Communication Media. Misrepresenting, obscuring, suppressing, or replacing a user's identity on any Communication Media is prohibited. "Spoofing" (constructing electronic communications so that it appears to be from someone else) is prohibited. The user name, electronic mail address, organizational affiliation, time and date of transmission, and related information included with messages or postings must always reflect the true originator, time, date and place of origination, of the message or postings, as well as the true content of the original message.

Employees may not use the email, voicemail, Internet computer network systems, or City-issued cell phone or any other City-issued electronic device in any way that is defamatory, obscene, or harassing or in violation of any City rules or policy. Examples of forbidden transmissions or downloads include sexually-explicit messages; unwelcome propositions; ethnic or racial slurs; or any other message that can be construed to be harassment or disparaging to others based on their actual or perceived age, race, religion, sex, sexual orientation, gender identity or expression, genetic information, disability, national origin, ethnicity, citizenship, marital status or any other legally recognized protected basis under federal, state or local laws, regulations or ordinances.

All employees, who have been granted access to electronically-stored data, must use a logon ID assigned by a Data Manager or Security Administrator. Employees must use an electronic "password" in conjunction with their logon ID to gain access to electronically-stored data. Certain data, or applications that process data, may require additional security measures as determined by the Security Administrator. Employees must not share their passwords; and each data user is responsible for all activity that occurs in connection with their passwords.

Procedures (continued):

Employees must not disable anti-virus and other implemented security software for receiving data from external providers and other employees, in order to minimize the risk of introducing computer viruses into the City's computing environment.

Employees may not install or modify ANY hardware device, software application, program code, either active or passive, or a portion thereof, without the express written permission from a Data Manager or Security Administrator. Employees may not upload, download, or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the City, or licensed to the City. Employees shall observe the copyright and licensing restrictions of all software applications and shall not copy software from internal or external sources unless legally authorized.

Monitoring: Because the City provides email, voicemail, Internet, cell phones and computer network systems to assist employees in performing their jobs, employees should use them for official business. The City reserves the right to access and disclose as necessary all messages sent over its systems, without regard to content, including employee blogging and social networking activity. Employees should not use any City Communication Media to transmit any message they would not want to disclose to a third party.

On-duty use of social media: Employees may engage in social media activity during work time, provided that it is directly related to their work.

Off-duty use of social media: Employees may maintain personal websites or blogs on their own time, using their own facilities. In general, the City considers social media activities to be personal endeavors, and employees may use them to express their thoughts or promote their ideas as long as they do not violate City rules or policies.

Prohibited material on social media: Employees are accountable for their actions and statements which have an impact on others. A social media site is a public place. Even if a message is posted anonymously, it may be possible to trace it back to the sender.

Employees must not make comments or otherwise communicate about coworkers, supervisors, managers, department heads, members of the governing body, vendors, suppliers, residents or any other third party with whom they interact in the course of the work day in a manner that violates City policy or rules or that is vulgar, obscene, threatening, intimidating, harassing, libelous or discriminatory on the basis of (actual

Procedures (continued):

or perceived) age, race, religion, sex, sexual orientation, gender identity or expression, genetic information, disability, national origin, ethnicity, citizenship, marital status or any other legally recognized protected basis under federal, state or local laws, regulations or ordinances. Those communications are disrespectful and unprofessional and will not be tolerated by the City.

Employees must respect the laws regarding copyrights, trademarks, rights of publicity and other third-party rights. To minimize the risk of a copyright violation, employees should provide references to the source(s) of information used and cite copyrighted works identified in online communications.

Post disclaimers: If employees identify themselves as City employees, or if they discuss matters related to the City on a social media site, the site must include a disclaimer on the front page, stating that it does not express the views of the City, and the employee is expressing only their personal views. For example: "The views expressed on this website/web log are mine alone and do not necessarily reflect the views of my employer." Place the disclaimer in a prominent position and repeat it for each posting that is expressing an opinion related to the City or the City's business. Employees must keep in mind that, if they post information on a social media site that is in violation of City policy and/or federal, state or local laws, the disclaimer will not shield them from disciplinary action.

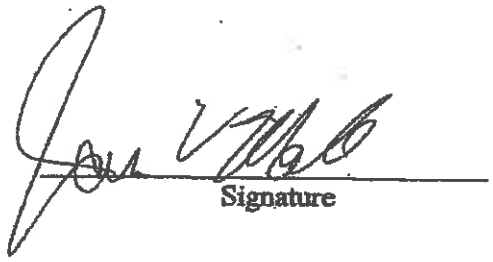
Social media and confidentiality: Employees must not reveal or publicize confidential information, including but not limited to personnel information, such as medical records or related information. When in doubt, ask before publishing.

Nothing in these policies is designed to interfere with, restrain or prevent employee communications regarding wages, hours or other terms and conditions of employment. City employees have the right to engage in or refrain from such activities.

Violations of the City's policies on the use of email, voicemail, Internet, complete network systems and City-issued cell phone, or any other City-issued electronic device, or the use of social media will subject the employee to discipline, up to and including immediate termination.

Acknowledgement: I have read and understand these policies. I have been given an opportunity to ask questions if there is something that I do not understand.

James V. Mallon
Print Name


Signature

5/29/14
Date