EMPLOYEE ACKNOWLEDGEMENT

1. **SOCIAL MEDIA POLICIES & GUIDELINES – Department; Employee**
2. **INFORMATION SYSTEMS ACCEPTABLE USE AGREEMENT - Revised**

I, the undersigned employee of the City of South Portland, have been provided a copy of the a.) City of South Portland Employee Use of Social Media Policy & Guidelines, dated July 30, 2013; and, b.) City of South Portland Social Media Use Policy for Departments, dated July 30, 2013; and, c.) Information Systems Acceptable Use Agreement, Revised July 30, 2013. I agree to review and fully comply with each of these policies. I accept and understand the terms of these policies and agree to abide by all terms contained in it.

____
Employee
Print Name: __________________________

Employee Signature:
____

____
Date

City of South Portland
Employee Use of Social Media Policy & Guidelines

At the City of South Portland (the "City"), we understand that social media can be a fun and rewarding way to share your life and opinions with family, friends and co-workers around the country. However, use of social media also presents certain risks and carries with it certain responsibilities. To assist you in making responsible decisions about your use of social media, we have established this Policy & Guidelines for appropriate use of social media.

POLICY & GUIDELINES

In the rapidly expanding world of electronic communication, *social media* can mean many things. *Social media* includes all means of communicating or posting information or content of any sort on the Internet, including to your own or someone else's web log or blog, journal or diary, personal web site, social networking or affinity web site, web bulletin board or a chat room, whether or not associated or affiliated with the City, as well as any other form of electronic communication.

Ultimately, you are solely responsible for what you post online. Before creating online content, consider some of the risks and rewards that are involved. What you write or post is public, and will be so for a long time. It will also be spread to large audiences without your knowledge or permission. Recognize that the instantaneous, yet permanent, nature of social media can pose risk without effective controls.

Know and follow the rules

Carefully read this Policy & Guidelines, the City's Personnel Policy, including the provisions on Employee Conduct, No Discrimination, Workplace Violence, Sexual and Anti-Harassment Prevention and Anti-Retaliation, and the City's Information Systems Acceptable Use Agreement, and ensure your postings are consistent with this Policy & Guidelines. Inappropriate postings that may include discriminatory remarks, harassment, and threats of violence or similar inappropriate or unlawful conduct will not be tolerated.

POLICY FOR ALL SOCIAL MEDIA COMMUNICATIONS

Use of social media on work time/equipment

Use social media while on work time or on equipment we provide must be work-related *and* approved by your Department Head or Supervisor; provided, however, that use of social media on work time or work equipment for personal reasons may be approved by your Department Head or Supervisor on a very limited basis and provided that it doesn't interfere with normal work. Be advised that employees have no right to privacy with respect to personal use of social media or personal social media accounts accessed by means of City equipment or with respect to personal social media content so accessed. Employees should not expect or assume privacy or confidentiality with respect to any such personal social media use or social media content.

Use of City name/e-mail address
Personal social media account names or e-mail names should not be tied to the City. Do not use a City e-mail address to register on social networks, blogs or other online tools utilized for personal use. For those employees who use a City e-mail address for registration with social networks, blogs or other online tools utilized for personal use as of the date of adoption of this Policy & Guidelines.

Protection of private and confidential information
Many City employees have access to private and confidential information that must be actively guarded from publication. When using social media, all City employees are expected to actively protect private and/or confidential information. A good rule of thumb is that if you are not sure if the information is protected as confidential by law, ask before you post.

Guidelines for all communications (official and personal)
All City employees have a responsibility to help communicate accurate and timely information to the public in a professional manner. Any employee who identifies a mistake in reporting should bring the error to the attention of his or her Supervisor or other appropriate staff. Employees must provide good customer service to both the public and co-workers. Regardless of whether the communication is in the employee's official City role or in a personal capacity, employees must comply with all laws relating to intellectual property rights, including, without limitation, trademark, copyright and software use. Employees must also follow all City policies that may apply.

Be mindful of public record and record retention laws
Maine's Freedom of Access Act ("Right-to-Know" law), State Archives Advisory Board Rules for Disposition of Local Government Records and e-discovery laws apply to social media content. Therefore, content must be able to be managed, stored and retrieved to comply with these laws.

Violations
Users who violate this Policy may be subject to discipline, up to and including termination of employment. This Policy is not intended to violate and will not be enforced in violation of federal, state or local law.

<u>GUIDELINES FOR PERSONAL USE OF SOCIAL MEDIA</u>
Some personal communications of employees may reflect on the City, especially if employees are commenting on City business, policies or fellow employees. These guidelines apply to personal communications involving various forms of social media. To assist you in making responsible decisions about your use of social media, we have established these guidelines for appropriate personal use of social media.

Be respectful
Always be fair and courteous to fellow employees and people who work on behalf of the City. Also, keep in mind that you are more likely to resolve work related complaints by speaking directly with your co-workers or your Supervisor than by posting complaints to a social media outlet. Nevertheless, if you decide to post complaints or criticism, avoid using statements,

photographs, video or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating, that disparage fellow employees and people who work on behalf of the City, or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law.

Be honest and accurate

Make sure you are always honest and accurate when posting information or news, and if you make a mistake, correct it quickly. Be open about any previous posts you have altered. Remember that the Internet archives almost everything; therefore, even deleted postings can be searched. Do not post any information or rumors that you know to be false about the City, its officials, fellow employees or people working on behalf of the City.

Post only appropriate and respectful content

- Maintain the confidentiality of information made confidential by law to which you have access solely as a result of your employment with the City.
- Do not create a link from your blog, website or other social networking site to the City's website without identifying yourself as a City employee.
- Express only your personal opinions. Never represent yourself as a spokesperson for the City. If the City is a subject of the content you are creating, be clear and open about the fact that you are an employee and make it clear that your views do not represent those of the City, its officials, fellow employees or people working on behalf of the City. If you do publish a blog or post online related to the work you do or subjects associated with the City, make it clear that you are not speaking on behalf of the City. It is best to include a disclaimer such as "The postings on this site are my own and do not necessarily reflect the views of my employer, the City of South Portland."
- For safety and security reasons, City employees are cautioned not to display City logos, uniforms, or similar identifying items on personal web pages.

Be mindful of public record and record retention laws

Maine's Freedom of Access Act ("Right-to-Know" law), State Archives Advisory Board Rules for Disposition of Local Government Records and e-discovery laws apply to social media content. Beware that even your personal social media content may be treated as a "public record" if it has "been received or prepared for use in connection with the transaction of public or governmental business or contains information relating to the transaction of public or governmental business." *See* 1 M.R.S.A. § 402(3).

FOR MORE INFORMATION

If you have questions or need further guidance on this Policy & Guidelines, please contact your Department Head, your Supervisor, the Information Technology Director or the Human Resources Director.

EMPLOYEE ACKNOWLEDGEMENT
SOCIAL MEDIA POLICY & GUIDELINES

I, the undersigned employee of the City of South Portland, have been provided a copy of the City of South Portland Employee Use of Social Media Policy & Guidelines and understand its contents fully. I accept and understand the terms of the policy and agree to abide by all terms contained in it.

____
Employee
Print Name: __________________________

____
Date

Information Systems Acceptable Use Agreement		
Policy #: 27	**Effective Date: 2/1/07**	**Change Control #:**
ISO/IEC 17799:2005 Reference:	6.1.5, 7.1.3, 8.1.3, 10.8.4, 11.3.2, 11.7.1, 11.7.2, 15.1.5	
Policy Overview:	The purpose of this policy is to protect the assets of the organization by clearly informing workforce members of their roles and responsibilities for utilizing the organizations information technology assets and infrastructure.	

The City of South Portland is committed to protecting the information assets of our residents, our employees, our partners and the City itself from illegal or damaging actions by individuals, either knowingly or unknowingly. Our intention for publishing our Information System Code of Conduct is not to impose restrictions that are contrary to our established culture of openness, trust and integrity but to ensure that we honor the public trust.

The 21st Century environment of connected technologies offers many opportunities to malicious or unknowing people from all over the world to anonymously attack, damage and corrupt vital public information; and to disrupt our ability to communicate effectively and accomplish the mission of our organization. Effective security is a civic responsibility, and a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every employee and affiliate to know, understand and adhere to these policies, standards, procedures, and guidelines, and to conduct their activities accordingly.

Distribution:
Current employees shall receive and sign a copy of this agreement annually. New employees shall receive a copy of this agreement upon hire. Any employee who does not sign the acceptable use statement will have all access to information systems immediately removed and may have their employment terminated.

Code of Conduct Agreement:

As an employee of the City of South Portland, I agree to protect the confidential information with which our residents entrust us in accordance with all Information Security Policies of the City of South Portland.

I certify that I have read and fully understand the Information Systems Code of Conduct set forth in this document. I understand and acknowledge my obligations and responsibilities.

I understand that should I become aware of any misuse of the City’s systems, I am obligated to inform a member of management immediately.

I understand that the City reserves the right to monitor system activity and usage. My signature on this document means I have consented to this monitoring.

I understand that electronic files created, sent, received, or stored on Information Systems owned, leased, administered, or otherwise under the custody and control of the City are not private and may be accessed City IS employees, management, or auditors at any time without my knowledge.

I understand that the City owns the email system and the information transmitted and stored within it. Employees shall have no expectation of privacy or confidentiality in any of their emails.

I understand that the City monitors Internet usage and that employees shall have no expectation of privacy or confidentiality for any information accessed via and/or published to the Internet via City information resources.

I further understand that violation of these policies is subject to disciplinary action up to and including termination without prior warning or notice. Additionally, individuals may be subject to civil and criminal prosecution.

Acknowledged and agreed to by: ____
Employee Signature Date

NAME (Printed): ____

Please complete and send this form to HR.

Information Systems Acceptable Use Agreement

January 2007

Please Retain this Document in a Convenient to Consult Location

Acceptable use of Information Resources policy
These rules are in place to protect our residents, our employees and the City. Inappropriate use of our Information Resources exposes the City to risks including virus attacks, compromise of network systems and services, and legal issues. City resources are made available to employees to conduct official business. City information resources are not to be used to conduct personal business, business related to outside employment or for personal benefit. System users are advised that there should be no expectation of privacy when using any City information resources. Every system user is expected to comply with this policy.

In order to insure safety and security of information assets:

1.1 Users must not share their user account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authentication purposes.

1.2 Users must not attempt to access any data or programs contained on information systems for which they do not have authorization or explicit consent.

1.3 In the event that a system user is sent, delivered or inadvertently accesses inappropriate or prohibited material, or the material contains confidential information that the user does not have "need-to-know" access to, or authority to receive; the user is required to immediately secure the material from view and notify their supervisor.

1.4 Users must not make unauthorized copies of copyrighted software.

1.5 Users must not install software, shareware or freeware software including games.

1.6 Users must not attempt to circumvent approved anti-virus software or make any changes to the accepted configuration of anti-virus software.

1.7 Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system.

1.8 Users must report any weaknesses in computer security, any incidents of possible misuse or violation of this agreement to their supervisor.

1.9 The distribution of any information through the Intranet, Internet, computer-based services, email, and messaging systems is subject to the scrutiny of the City and or its auditors. The City reserves the right to determine the suitability of this information.

2. Internet Use

In addition to being an excellent resource for information, and a revolutionary way to communicate with the world; The Internet is a rapidly changing and volatile place which can accurately be referred to as "The Wild". These policies are intended to provide guidance and protection, while still making available this useful business tool.

The following rules apply when using the Internet:

2.1 Users must not - upload, download, or otherwise knowingly access or transmit in any fashion any confidential records of the City, its residents, or vendors without adequate authority to do so. Employees must know what is and is not acceptable based on their position and function within the City. Without limiting the foregoing, Users must be aware of and comply with City of South Portland's privacy policy, and policies and procedures for safeguarding information.

2.2 All authorized confidential information transmitted via the Internet – email, FTP, or otherwise, must be encrypted or secured in a manner approved by the City management.

2.3 Users must not knowingly visit Internet sites that contain obscene, hateful or other objectionable materials; send or receive any material, whether by email, voice mail, memoranda or oral conversation, that is obscene, defamatory, harassing, intimidating, offensive, discriminatory, or which is intended to annoy, harass, or intimidate another person.

2.4 Users must not solicit business for personal gain or profit via the City Information Services infrastructure.

2.5 Users must not use the Internet or email for any illegal purpose.

2.6 Users must not use the Internet or email for offensive or vulgar messages such as messages that contain sexual or racial comments or for any messages that do not conform to the City's policies against harassment and discrimination.

2.7 Users must not download or install any software or electronic files without the prior written approval of the IS Director.

2.8 Users must not access the Internet via any means other than a City approved connection.

2.9 Users must not change any security settings in Internet Explorer unless under the direction of the IS department.

2.10 Users must not participate in unauthorized activities.

2.11 Users must not represent personal opinions as those of the City or purport to represent the City when not authorized to do so.

2.12 Users must not upload, download, or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the City.

2.13 Users must not intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic, which substantially hinders others in their use of the network.

2.14 Users must not reveal or publicize confidential or proprietary information which includes, but is not limited to: financial information, confidential client information, marketing strategies and plans, databases and any information contained therein, client lists, computer software source codes, computer/network access codes, and business relationships.

3. Email Use

Email use has become a standard method of communication. These policies are intended to offer rules of usage which will protect our information. Email use is subject to the following policies:

3.1 The City owns the email system and the information transmitted and stored within it. Employees should have no expectations of privacy.

3.2 All confidential information sent via email must use a designated secure email system.

3.3 The following activities are prohibited:

3.3.1 Sending email that is intimidating or harassing.
3.3.2 Using email for purposes of political lobbying or campaigning.
3.3.3 Violating copyright laws by inappropriately distributing protected works.
3.3.4 Posing as anyone other than oneself when sending or receiving email, except when authorized to send messages for another when serving in an administrative support role.

3.4 The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:

3.4.1 Sending or forwarding chain letters.
3.4.2 Sending unsolicited messages to large groups except as required to conduct agency business.
3.4.3 Sending excessively large messages.
3.4.4 Sending or forwarding email that is likely to contain computer viruses.

3.5 Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the City.

3.6 Individuals must not send, forward or receive confidential or sensitive information through non-City email accounts. Examples of non-City email accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, and email provided by other Internet Service Providers (ISP).

3.7 Individuals must not send, forward, receive or store confidential or sensitive information utilizing non-City accredited mobile devices. Examples of mobile devices include, but are not limited to, Personal Data Assistants, Palm Pilots, Blackberries, iPods, two-way pagers and cellular telephones.

3.8 Email messages are not private but are property of the City. The City may print and review email messages sent and received via an employee's email account.

3.9 Internet sites accessed from City resources are not private and the City may review the sites visited.

4. Incidental Use of Information Resources

As a convenience to the user community, incidental use of Information Resources is permitted. Only brief and occasional use is considered to be incidental. All rules that apply to official use of information resources also apply to incidental usage as outlined above.

The following additional restrictions on incidental use apply:

Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, and so on, is restricted to approved users; it does not extend to family members or other acquaintances.

Incidental use must not result in direct costs to the City.

Incidental use must not interfere with the normal performance of an employee's work duties.

Incidental use of information resources must not involve solicitation in any form, must not be associated with any outside business or employment activity, and must not potentially embarrass or offend the City, its Council Members, its Residents, or its Employees.

All messages, files and documents – including personal messages, files and documents – located on information resources are considered to be owned by the City and may be subject to open records requests, and may be accessed in accordance with this policy.

5. Passwords

All of the work we are doing at the City of South Portland to secure the confidential information will be ineffective if the most important aspect of Information Security, the users of our information resources, have weak passwords. Though we recognize that it is inconvenient at first, having strong passwords is the most important part of your participation. We would like to think of passwords as a "shared secret" between you and the City information resources.

The following policies apply to password use:

5.1 All passwords must be constructed and implemented according to the City's accepted and approved standards.

5.2 User account passwords must not be divulged to anyone, at any time, for any reason.

5.3 If passwords are forgotten, disclosed, or if the security of a password is in doubt, the password must be changed immediately.

5.4 Administrators may not circumvent the Password Policy for the sake of ease of use.

5.5 Users must not circumvent password entry with auto logon, password remembering features, embedded scripts or hard-coded passwords in client software.

5.6 Computing devices must not be left unattended without enabling a password protected screensaver, locking the workstation or completely logging off of the device.

5.7 In the event passwords are found or discovered on documents of any kind, the following steps must be taken:

5.7.1 Take possession of the passwords and protect them,

5.7.2 Report the discovery to the Helpdesk,
5.7.3 Transfer the passwords to an authorized person as directed by the Helpdesk.

6. Remote Computing

Laptop computers, PDA's, and other portable computing devices are a great convenience and becoming more and more a part of doing business. They also come with many risks including ease of theft, operation in unsecured environments, and easily intercepted wireless communications. In order to protect our valuable information; it is important that users of portable computing devices follow these rules of use:

6.1 Only City approved portable computing devices may be used to access City information resources.

6.2 Portable devices are assigned to individual employees. Portable devices should not be used by any employee other than one to whom the device is assigned.

6.3 Physical security of portable computing devices is the responsibility of the user.

6.4 Lost or stolen portable devices must be reported to the IS department immediately.

6.5 Confidential / sensitive information must not be saved onto portable computing devices.

6.6 Remote connection to the City's network resources must only be done via approved access methods (i.e. VPN).

6.7 When left unattended, portable computing devices shall not be left logged into the City's network and/or have implemented a password protected screen saver to prevent unauthorized access.

7. Media Handling

Removable electronic storage media (floppy disks, CD's, DVD's, USB drives, flash drives, Zip disks, etc.) are evolving to where they can store an enormous amount of data on a very small device. This presents a unique challenge to organizations as the devices are difficult to secure. In order to protect our valuable information; it is important that users of electronic storage media follow these rules of use:

7.1 Confidential / sensitive information shall not be saved onto removable electronic media without approval from the IS manager. If approved, the information must be encrypted prior to being saved onto removable electronic media.

7.2 Removable media that contains (or previously contained) confidential / sensitive information shall be provided to the IS department to ensure that it has been "wiped" securely prior to reuse and/or disposal.

7.3 Removable media that contains (or previously contained) confidential / sensitive information shall not be shared with individuals that do not have a "need-to-know" of the information.

7.4 Removable media that contains (or previously contained) confidential / sensitive information shall be kept physically secure (in a locked cabinet and/or office) when not in use.

Enforcement:

Violations of this policy may result in disciplinary action. Depending on the severity or frequency of the violations, this could include:

1. Counseling statements for policy violations.
2. A suspension / termination of Internet or email privileges. This could then result in a position / function reassignment, and the employee's compensation package may be affected.
3. A termination of employment.
4. Personal liability under applicable local, state, or international laws.

Internal audits will be completed upon the request of management. It will investigate any breach of this policy and any enforcement will follow regular personnel procedures.

Standard Definitions:

Information Resources:
Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, telecommunication resources including cell phones and voice mail systems, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Remote Computing Device:
Any easily portable device that is capable of receiving and/or transmitting data to and from City information resources. These include, but are not limited to, notebook computers, handheld computers, PDAs, pagers, and cell phones.

Electronic mail (email):
Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

Internet:
A global system inter-connecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges. The Internet is the present "information super highway."

Intranet:
A private network for communications and sharing of information that, like the Internet, is based on TCP/IP, but is accessible only to authorized users within an organization. An organization's intranet is usually protected from external access by a firewall.

World Wide Web:
A system of Internet hosts that supports documents formatted in HTML (Hypertext Markup Language) which contain links to other documents (hyperlinks) and to audio, video, and graphic images. Users can access the Web with special applications called browsers, such as Netscape Navigator and Microsoft Internet Explorer.