City Council Workshop | Agenda Item #3

February 8, 2016 | iPad Policy

The South Portland City Council iPad Policy outlines the usage agreement for City Councilors of City-issued iPads. iPads are issued to City Councilors primarily as a tool for conducting city business, including receiving City Council agendas and packet information, staff reports, and connecting to the Internet and city e-mail.

The iPad Policy ø l·ă fl·ăű ʤLJŘl·ΰŜŘ ỉy ̃September 2011. The policy predates the current Information Technology (IT) director. Based on feedback, staff is making the recommendation that the policy be updated to reflect technology changes, the terms and conditions for appeals for the replacement for lost or stolen property, and the terms and conditions for the return or purchase of the iPad at the end of a Councilor's service. A draft of the updated iPad Policy is included in the workshop packet for consideration by the Council (changes to the original policy have been red-lined and highlighted).

The Council may wish to further amend the policy and/or address concerns or questions related to accountability and enforcement, and the definition of "city business" brought forward by an individual councilor.

Other existing IT-related city policies (City Council Electronic Communications Protocol, Social Media Policy, and Information Systems Acceptable Use Agreement) referenced in the iPad Policy (Sec. 5, paragraph 2) are being included in the workshop packet for reference.

February 1, 2016

South Portland City Council iPad Policy

Section 1. Purpose

The City Council acknowledges and agrees that the provision and use of an iPad will assist the members of the City Council in the efficient performance of their duties as City Councilors and thereby improve their service to the public. The use of the iPad will also reduce paper and photocopying costs. This policy is adopted by the City Council and constitutes its mutual statement of what are, and are not, appropriate uses for this important technology tool.

The explicit privileges and restrictions set forth in this policy do not attempt to cover every situation that may arise in connection with the use of this new form of electronic communication. City Councilors acknowledge, understand and respect the underlying iPad, Internet and usage philosophy that forms the basis of this policy, including the understanding that only the City e-mail account will be used to conduct City business and that the City will no longer provide paper meeting packets to City Councilors. (One hard copy of the paper meeting packet will still be available at every City Council meeting.)

Section 2. Receipt of iPad

The City's Information Technology (IT) Department will issue City Councilors an iPad ~~with 3G technology installed and a cover or case. (Any additional iPad accessories, such as keyboards,~~ with Wi-Fi technology installed case or keyboard case. (Any additional iPad accessories, such as keyboards (if not included with the case), styluses, screen protectors, cables or adapters, shall be at the individual City Councilor's own expense and shall remain the property of the City Councilor at the end of the Councilor's term and service.) City Councilors have already or will each receive a separate e-mail account that shall be used to send City Councilors official City documents, including, without limitation, City Council agendas, staff reports, packets and the like as well as for City Councilors to send all e-mails relating to City business. The iPad will serve as the City Councilors' sole source of meeting packets; paper meeting packets will not be provided to City Councilors. City Councilors will have access to the Internet through the iPad. Before being authorized to access and utilize City computer and iPad equipment for Internet and e-mail communication, a City Councilor shall sign the City's iPad Agreement, a copy of which is attached hereto and incorporated herein.

Section 3. Care of iPad

City Councilors are responsible for the general care of the iPad that they have been issued by the City. iPads that are broken or fail to work property must be taken to the IT Department for an evaluation of the equipment. iPads must remain free of any writing, drawing, stickers or labels that are not the property of the City. Only a clean, soft cloth should be used to clean the screen.

Section 4. Software on iPad

The software and applications installed by the City must remain on the iPad in usable condition and be readily accessible at all times. From time to time, the City may add or upgrade software applications for use by City Councilors such that City Councilors may be required to check in their iPads with the IT Department for periodic updates and synching. Any software, e-mail messages or files downloaded via the Internet into the City systems become the property of the City and may only be used in ways that are consistent with applicable licenses, trademarks or copyrights.

Files from sources that a City Councilor may have any reason to believe may be untrustworthy shall not be downloaded, nor shall files attached to e-mail transmissions be opened and read unless the City Councilor has knowledge that they originate from a trustworthy source. Downloaded files and attachments may contain viruses or hostile applications that could damage the City's information systems. City Councilors will be held accountable for any breaches of security caused by files obtained for non-City business purposes.

If technical difficulties occur or illegal software is discovered, the iPad will be restored from backup. The City does not accept responsibility for the loss of any software or documents deleted due to a re-format and re-image.

Section 5. Acceptable Use

The iPad, Internet and e-mail access provided are tools for conducting City business. Thus, City Councilors use of such tools will be primarily for City business related purposes, *i.e.*, to review City Council agenda materials, obtain useful information for City related business and conduct City related business communications as appropriate. All of the City's computer systems, including the iPad, are considered to be public property. All documents, files and e-mail messages created, received, stored in, or sent from any City iPad are considered public records, subject to disclosure to the public pursuant to the Maine Freedom of Access Act (with only limited exceptions), and are considered the property of the City of South Portland.

All existing City policies will continue to apply to City Councilor conduct on the Internet and in the use of e-mail, including, but not limited to those that deal with misuse of City resources, sexual harassment, electronic communications, information and data security, and confidentiality. iPad, Internet and e-mail activities will be traceable to the City of South Portland and will impact the reputation of the City. City Councilors are to refrain from making any false or defamatory statements in any Internet forum or from committing any other acts that could expose the City to liability.

City Councilors shall not use e-mail, instant messaging, text messaging or similar forms of electronic communications at any time during a meeting of the City Council at which he or she is in attendance. This limitation shall not apply to receipt of communications from family members in the event of an urgent family matter; a City Councilor wishing to respond to such a message during the meeting shall do so during a recess or shall excuse him or herself from the meeting to place a response to the message in a manner that does not disrupt the meeting. City

Councilors shall not use the iPad in any way as to violate the public meeting requirements of the Maine Freedom of Access Act.

City Councilors shall not use City issued iPads for operating a business for personal gain, sending chain letters, soliciting money for religious or political causes, or any or other purpose that interferes with normal City business activities. City Councilors shall not use City issued iPads for any illegal activity.

City Councilors shall not use City issued iPads to deliberately propagate any virus or other hostile computer program or file, to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

Section 6. Repairing and Replacing iPad

iPads that malfunction or are damaged must be reported to the IT Department. The City will be responsible for repairing iPads that malfunction. iPads that have been damaged from misuse or neglect, in the sole and exclusive judgment of the IT Director, will be repaired by the City, with the cost borne by the City Councilor. Damage includes, but is not limited to, broken screens, cracked plastic pieces, and inoperability. If the cost to repair the iPad exceeds the cost of purchasing a new device, the City Councilor shall pay the full replacement value. ~~If the iPad is stolen or lost, the City Councilor shall pay an amount deemed appropriate by the balance of the City Council.~~ If the iPad is stolen or lost, the City Councilor shall pay the full amount of the replacement. All appeals will be decided by the balance of the City Council.

Section 7. Return or Purchase of iPad

~~City Councilors shall return their iPad to the IT Department when the individual Councilor's term and service on the City Council has ended. Upon return of the iPad to the City and following the preparation of any appropriate backup files, the iPad will be wiped clean of any and all information at the end of a Councilor's term and service.~~ City Councilors will be given the choice to purchase their iPad for its market value deemed by the City IT Director or return their iPad to the IT Department when the individual Councilor's term has ended. The City IT Department will backup files and wipe clean any and all information at the end of a Councilor's term and service.

Section 8. Compliance with Policy

The City reserves the right to inspect any and all files stored on iPads that are the property of the City in order to ensure compliance with this policy. City Councilors do not have any personal privacy right in any matter created, received, stored in, or sent from any City issued iPad, and the IT Director is hereby authorized to institute appropriate practices and procedures to ensure compliance with this policy.

Failure to comply with this or any other security policy may result in disciplinary actions as deemed appropriate by the balance of the City Council.

February 1, 2016

CITY OF SOUTH PORTLAND
IPAD AGREEMENT
FOR CITY COUNCIL MEMBERS

I, the undersigned City Councilor of the City of South Portland, have been provided a copy of the City of South Portland iPad Policy and understand its contents fully. I accept and understand the terms of the policy and agree to abide by all terms contained in it.

City Councilor
Print Name: _____

Date

Original: 9/7/11, Revised: 2/1/16

September 7, 2011

South Portland City Council iPad Policy

Section 1. Purpose

The City Council acknowledges and agrees that the provision and use of an iPad will assist the members of the City Council in the efficient performance of their duties as City Councilors and thereby improve their service to the public. The use of the iPad will also reduce paper and photocopying costs. This policy is adopted by the City Council and constitutes its mutual statement of what are, and are not, appropriate uses for this important technology tool.

The explicit privileges and restrictions set forth in this policy do not attempt to cover every situation that may arise in connection with the use of this new form of electronic communication. City Councilors acknowledge, understand and respect the underlying iPad, Internet and usage philosophy that forms the basis of this policy, including the understanding that only the City e-mail account will be used to conduct City business and that the City will no longer provide paper meeting packets to City Councilors. (One hard copy of the paper meeting packet will still be available at every City Council meeting.)

Section 2. Receipt of iPad

The City's Information Technology (IT) Department will issue City Councilors an iPad with 3G technology installed and a cover or case. (Any additional iPad accessories, such as keyboards, styluses, screen protectors, cables or adapters, shall be at an individual City Councilor's own expense and shall remain the property of the City Councilor at the end of the Councilor's term and service.) City Councilors have already or will each receive a separate e-mail account that shall be used to send City Councilors official City documents, including, without limitation, City Council agendas, staff reports, packets and the like as well as for City Councilors to send all e-mails relating to City business. The iPad will serve as the City Councilors' sole source of meeting packets; paper meeting packets will not be provided to City Councilors. City Councilors will have access to the Internet through the iPad. Before being authorized to access and utilize City computer and iPad equipment for Internet and e-mail communication, a City Councilor shall sign the City's iPad Agreement, a copy of which is attached hereto and incorporated herein.

Section 3. Care of iPad

City Councilors are responsible for the general care of the iPad that they have been issued by the City. iPads that are broken or fail to work property must be taken to the IT Department for an evaluation of the equipment. iPads must remain free of any writing, drawing, stickers or labels that are not the property of the City. Only a clean, soft cloth should be used to clean the screen.

Section 4. Software on iPad

The software and applications installed by the City must remain on the iPad in usable condition and be readily accessible at all times. From time to time, the City may add or upgrade software applications for use by City Councilors such that City Councilors may be required to check in their iPads with the IT Department for periodic updates and synching. Any software, e-mail messages or files downloaded via the Internet into the City systems become the property of the City and may only be used in ways that are consistent with applicable licenses, trademarks or copyrights.

Files from sources that a City Councilor may have any reason to believe may be untrustworthy shall not be downloaded, nor shall files attached to e-mail transmissions be opened and read unless the City Councilor has knowledge that they originate from a trustworthy source. Downloaded files and attachments may contain viruses or hostile applications that could damage the City's information systems. City Councilors will be held accountable for any breaches of security caused by files obtained for non-City business purposes.

If technical difficulties occur or illegal software is discovered, the iPad will be restored from backup. The City does not accept responsibility for the loss of any software or documents deleted due to a re-format and re-image.

Section 5. Acceptable Use

The iPad, Internet and e-mail access provided are tools for conducting City business. Thus, City Councilors use of such tools will be primarily for City business related purposes, *i.e.*, to review City Council agenda materials, obtain useful information for City related business and conduct City related business communications as appropriate. All of the City's computer systems, including the iPad, are considered to be public property. All documents, files and e-mail messages created, received, stored in, or sent from any City iPad are considered public records, subject to disclosure to the public pursuant to the Maine Freedom of Access Act (with only limited exceptions), and are considered the property of the City of South Portland.

All existing City policies will continue to apply to City Councilor conduct on the Internet and in the use of e-mail, including, but not limited to those that deal with misuse of City resources, sexual harassment, electronic communications, information and data security, and confidentiality. iPad, Internet and e-mail activities will be traceable to the City of South Portland and will impact the reputation of the City. City Councilors are to refrain from making any false or defamatory statements in any Internet forum or from committing any other acts that could expose the City to liability.

City Councilors shall not use e-mail, instant messaging, text messaging or similar forms of electronic communications at any time during a meeting of the City Council at which he or she is in attendance. This limitation shall not apply to receipt of communications from family members in the event of an urgent family matter; a City Councilor wishing to respond to such a message during the meeting shall do so during a recess or shall excuse him or herself from the meeting to place a response to the message in a manner that does not disrupt the meeting. City

Councilors shall not use the iPad in any way as to violate the public meeting requirements of the Maine Freedom of Access Act.

City Councilors shall not use City issued iPads for operating a business for personal gain, sending chain letters, soliciting money for religious or political causes, or any or other purpose that interferes with normal City business activities. City Councilors shall not use City issued iPads for any illegal activity.

City Councilors shall not use City issued iPads to deliberately propagate any virus or other hostile computer program or file, to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

Section 6. Repairing and Replacing iPad

iPads that malfunction or are damaged must be reported to the IT Department. The City will be responsible for repairing iPads that malfunction. iPads that have been damaged from misuse, neglect or are accidentally damaged, in the sole and exclusive judgment of the IT Director, will be repaired by the City, with the cost borne by the City Councilor. Damage includes, but is not limited to, broken screens, cracked plastic pieces, and inoperability. If the cost to repair the iPad exceeds the cost of purchasing a new device, the City Councilor shall pay the full replacement value. If the iPad is stolen or lost, the City Councilor shall pay an amount deemed appropriate by the balance of the City Council.

Section 7. Return of iPad

City Councilors shall return their iPad to the IT Department when the individual Councilor's term and service on the City Council has ended. Upon return of the iPad to the City and following the preparation of any appropriate backup files, the iPad will be wiped clean of any and all information at the end of a Councilor's term and service.

Section 8. Compliance with Policy

The City reserves the right to inspect any and all files stored on iPads that are the property of the City in order to ensure compliance with this policy. City Councilors do not have any personal privacy right in any matter created, received, stored in, or sent from any City issued iPad, and the IT Director is hereby authorized to institute appropriate practices and procedures to ensure compliance with this policy.

Any violation of this policy may result in discipline as deemed appropriate by the balance of the City Council.

September 7, 2011

CITY OF SOUTH PORTLAND
IPAD AGREEMENT
FOR CITY COUNCIL MEMBERS

I, the undersigned City Councilor of the City of South Portland, have been provided a copy of the City of South Portland iPad Policy and understand its contents fully. I accept and understand the terms of the policy and agree to abide by all terms contained in it.

City Councilor
Print Name: _____

Date

August 19, 2011

South Portland City Council Electronic Communications Protocol

1. Electronic communication shall not be used to defeat purpose of the Maine's Freedom of Access ("Right-to-Know") law, which is to conduct the people's business in public with public notice of public meetings; the general public has the right to attend meetings of public bodies and to see and hear discussions of each public body. For purposes of this protocol, the term "electronic communication" means electronic text or visual communication and attachments distributed via e-mail, websites, instant messaging, text messaging, chat rooms, news groups, online forums, weblogs, twitter feeds, list serves, social networking sites or comparable services.

2. City Councilors have already or will each receive a separate e-mail account that shall be used to send City Councilors official City documents and shall be used by City Councilors to send all e-mails relating to City business. If a current or new City Councilor is transitioning to the exclusive use of the City of South Portland e-mail address for City business, during the transition phase, the City Councilor shall forward incoming e-mails to his/her City of South Portland e-mail address. Any response to the incoming e-mail shall be from the City Councilor's City of South Portland e-mail address with an explanatory note that the City Councilor conducts City business from a City of South Portland e-mail address and that all future correspondence should be sent to the City Councilor at the new City of South Portland e-mail address.

3. Three or more City Councilors or three or more members of any volunteer City board or committee shall avoid the use of electronic communication for deliberation, discussion or voting on matters properly confined to public meetings. E-mail should be used for non-substantive matters such as scheduling meetings, dissemination of information and reports, and developing agendas for future meetings.

4. E-mail or other forms of electronic communication shall not be used for any deliberation or discussion related to quasi-judicial matters (e.g., license and permit applications, general assistance fair hearings, poverty abatement applications). In the event a City Councilor receives an e-mail or other communication related to a quasi-judicial matter, the City Councilor should (a) advise the sender by return e-mail that he or she cannot comment outside a public meeting on the pending matter before the City Council and that the sender's e-mail is being forwarded to the City Manager for inclusion in the public record on the matter; (b) immediately forward the e-mail or other communication to the City Manager for inclusion in the public record of the matter; and (c) disclose on the record in the public hearing or meeting on the matter that the e-mail or other communication has been received and is in the record.

5. City Councilors shall not use electronic communication at any time during a meeting of the City Council at which he or she is in attendance. This limitation shall not apply to receipt of communications from family members in the event of an urgent family matter; a City Councilor wishing to respond to such a message during the meeting shall do so during a recess or shall excuse him or herself from the meeting to place a response to the message in a manner that does not disrupt the meeting.

6. In the event the protocols above are not followed, or if there is a question whether substantive matters properly confined to public meetings were discussed or deliberated on via e-mail or other forms of electronic communication by three or more members of any City body, those electronic communications in question should be printed and disclosed to the public at the next public meeting of the City body.

7. To the extent that City Councilors use e-mail for communications related to City business, a "cc" of each e-mail sent or received shall be sent to the City Council Inbox (address available from City Manager or IT Director). In addition, a public records/public meeting disclaimer should be included at the bottom of each e-mail as follows:

> NOTICE: Under Maine's Freedom of Access ("Right-to-Know") law, documents - including e-mail - in the possession of public officials about City business are classified as public records. This means if anyone asks to see it, we are required to provide it. There are very few exceptions. We welcome citizen comments and want to hear from our residents, but please keep in mind that what you write in an e-mail is not private and could show up in the local newspaper. Please also keep in mind that the City Council and volunteer City boards and committees cannot use e-mail for deliberation, discussion or voting on matters properly confined to public meetings.

8. The Mayor, or the Mayor's designated representative, shall acknowledge e-mail messages from the general public that come to all City Council members at once. While the Mayor is not empowered to discuss substantive matters on behalf of the City Council in these acknowledgements (*see* City Council Rule 22), he or she may, in consultation with staff if necessary, supply pertinent information regarding how the City Council will proceed with the issue, if applicable (for example, upcoming public hearings, information available through the City's website, and so on). The Mayor and individual City Councilors remain free to reply to such messages as individuals, but shall refrain from engaging more than one other City Councilor in the electronic discussion.

9. If a City Councilor receives an e-mail from the general public addressed to less than the entire City Council, the recipient may (a) treat it as an individual communication to which he or she may or may not respond; (b) inform the City Council of the

communication at a properly noticed meeting; or (c) forward it to the City Manager and ask that it be forwarded to the entire City Council. Such an e-mail may also be forwarded to staff for a response.

10. If the City Council as a whole or an individual City Councilor receives an e-mail or other correspondence relating to a current agenda item from a member of the general public who requests that the correspondence be "read into the record" at a future City Council meeting, the Mayor or individual recipient, as applicable, may briefly summarize the content of the correspondence during consideration of that agenda item.

11. City Councilors shall exercise caution in sending confidential information by e-mail or other form of electronic communication because of the ease in which such information can lose confidentiality by inadvertent or intentional diversion or re-transmission by others.

12. Under Right-to-Know law, all e-mail and e-mail attachments received or prepared for use in matters concerning City business or containing information relating to City business are likely to be regarded as public records that may be inspected by any person upon request, unless otherwise made confidential by law. All e-mail and e-mail attachments are also subject to the "record retention requirements" of State law.

Information Systems Acceptable Use Agreement		
Policy #: 27	**Effective Date: 2/1/07** **Revised Date: 5/22/13**	**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 City" by clearly informing workforce members of their roles and responsibilities for utilizing the City's 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.

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 and contractors shall receive and sign a copy of this agreement annually. New employees shall receive a copy of this agreement upon hire. Any employee or contractor 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 or contractor 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 and that 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 by City IT 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

May 22, 2013

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 expose 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 business related to outside employment or for personal benefit unless otherwise noted. 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. 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:

2.1 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.

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

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

2.4 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.

2.5 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.

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, harassing, sexually explicit, vulgar, or illegal.
- 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 Email 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 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.

4. Internet Use

The City of South Portland provides computer systems that allow access to the Internet in order to facilitate the effective and efficient conduct of City of South Portland business. Users are permitted access to the Internet and electronic communication systems to assist in the performance of their jobs. Internet Use is subject to the following policies:

4.1 Users must not upload, download, or otherwise knowingly access or transmit 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.

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

4.3 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.

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

4.5 Users must not use the Internet for any illegal purpose.

4.6 Users must not download or install any software or electronic files without the prior written approval of the City Information Technology Director..

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

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

4.9 Users must not participate in unauthorized activities.

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

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

4.12 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.

4.13 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.

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 Passwords must be at least 8 characters in length
5.2 Passwords must be a mixture of upper case letters, lower case letters, special characters and numbers
5.3 Passwords must be changed at least every 90 days
5.4 Passwords must be different from the previous 6 passwords
5.5 Passwords must not contain the user's user id

5.6 Passwords must not be divulged by any means, to anyone, at any time, for any reason.

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

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

5.9 Users must not circumvent password entry with auto logon, password remembering features, embedded scripts or hard-coded passwords in client software, unless approved by the IT Director.

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

5.10.1 Take possession of the passwords and protect them,
5.10.2 Report the discovery to the Helpdesk,
5.10.3 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 The Remote Access Request Form must be filled out and signed before access is granted.
6.2 Only City approved portable computing devices may be used to access City information resources.

6.3 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.
6.4 Do not allow unauthorized individuals to access or view City of South Portland information, especially confidential information
6.5 Physical security of portable computing devices is the responsibility of the user.
6.6 Lost or stolen portable devices must be reported to the IT department immediately.
6.7 Confidential / sensitive information must not be saved onto portable computing devices.
6.8 Remote connection to the City's network resources must only be done via approved access methods (i.e. VPN).
6.9 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. Cloud Computing

Cloud computing is a great convenience and becoming more and more a part of doing business. It also comes with many considerations including the potential breach of confidential data and Freedom of Access Act ("Right-to-Know" law) requests. The City only authorizes the use of Cloud Computing under specific guidelines. The following policies apply to Cloud Computing use:

7.1 Use of Cloud Computing services must comply with all current laws, IT security, and risk management policies

7.2 Use of Cloud Computing services must comply with all privacy laws and regulations, and appropriate language must be included in the vehicle defining the Cloud Computing source responsibilities for maintaining privacy requirements

7.3 For external Cloud Computing services that require users to agree to terms of service agreements, such agreements must be approved by the City Manager, in consultation with the Corporation Counsel

7.4 Use of Cloud Computing services must be formally authorized on a case-by-case, employee-by-employee basis in writing by the City's IT Director

7.5 The users of Cloud Computing must sign the Cloud Computing agreement and return to the IT Director

7.6 The City's IT Director reserves the right to terminate the use of existing Cloud Computing services as technology changes or more secure solutions become available.

8. Social Media

To address the fast-changing landscape of the Internet and the way the general public communicates and obtains information online, City of South Portland departments may consider using social media tools to reach a broader audience. The City has an overriding interest and expectation in deciding what is "spoken" on behalf of the City and the City's website (*www.southportland.org*) will remain the City's primary and predominant Internet presence. There are times where social media sites may be needed for a further outreach. Below is summary of City guidelines for the City's use of social media:

8.1 The use of RSS (Really Simple Syndication) feeds from the City Website, shall be the preferred method for dissemination of public information by the City.

8.2 No City employee or official may establish any social media identity, account, profile, page, or site (collectively, "social media account(s)") in the name of or on behalf of the City or any City department unless the City Manager or his designee, the IT Director and the Department Head have all approved the account.

8.3 Upon approval, Department Heads will be responsible for the content and upkeep of any social media accounts their department may create.

8.4 City social media accounts are subject to Maine's public records disclosure law, the Freedom of Access Act ("Right-to-Know" law). All Maine laws and relevant record retention schedules apply to social media formats and social media content. Therefore, if the content cannot meet these requirements, the use of social media will be prohibited.

8.5 The City reserves the right to restrict or remove any content that is deemed in violation of this Social Media Policy or any applicable law

8.6 The City will approach the use of social media tools as consistently as possible, enterprise-wide.

8.7 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 a complete copy of the City's social media policies and guidelines, please refer to (i) the City of South Portland Employee Use of Social Media Policy & Guidelines, and (ii) the City of South Portland Social Media Use Policy. Copes are available from the IT Director and the Human Resources Director.

9. Removable Media Handling

Removable electronic storage media (CD's, DVD's, USB drives, flash drives,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:

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

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

9.3 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.

9.4 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:

Failure to comply with this or any other security policy may result in disciplinary actions up to and including termination. Legal actions also may be taken for violations of applicable state and federal law. Please note that in certain circumstances where an employee acts outside the scope of their employment, and if not authorized, they risk exposing themselves to potential liability. The City may have no duty to defend or indemnify that employee for any subsequent claims against them. Accordingly, great care should be taken not to expose yourself to personal liability.
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, tablets, 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 Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome.

Purpose

To address the fast-changing landscape of the Internet and the way the general public communicates and obtains information online, City of South Portland departments may consider using social media tools to reach a broader audience. The City encourages the use of social media to further the goals of the City and the missions of its departments, where appropriate.

The City has an overriding interest and expectation in deciding what is "spoken" on behalf of the City on social media sites. This policy establishes guidelines for the City's use of social media.

Policy

1. The City's website (*www.southportland.org*) will remain the City's primary and predominant Internet presence.
    (a) The best, most appropriate City uses of social media tools fall generally into two categories:
        (i) As channels for disseminating time-sensitive information as quickly as possible (for example, emergency information).
        (ii) As marketing/promotional channels that increase the City's ability to broadcast its messages to the widest possible audience.
    (b) The use of RSS (Really Simple Syndication) feeds shall be the preferred method for dissemination of public information by the City.
    (c) Wherever possible, content posted to City social media accounts will also be available on the City's main website.
    (d) Wherever possible, content posted to City social media accounts should contain links directing users back to the City's official website for in-depth information, forms, documents or online services necessary to conduct business with the City.

2. No City employee, elected official, appointed official, contractor, department, board or committee may establish any social media identity, account, profile, page, or site (collectively, "social media account(s)") in the name of or on behalf of the City or any City department unless the City Manager or his designee, the IT Director and the Department Head, as appropriate, have all approved the account. This requirement applies regardless of whether the account is established, accessed, or used by means of City information systems or by means of the employee's or others' information systems, and regardless of whether the account is established, accessed, or used from City or non-City premises.

3. Following approval under Section 2 above, Department Heads will be responsible for the content and upkeep of any social media accounts their department may create.

4. All City social media accounts shall comply with all appropriate City policies and standards, including, but not limited to, the City's Personnel Policy and Information Systems Acceptable Use Agreement.

5. City social media accounts are subject to Maine's public records disclosure law, the Freedom of Access Act ("Right-to-Know" law). Any content maintained in a social media

format that is related to City business is a public record. The department maintaining the account is responsible for responding completely and accurately to any public records request for public records on social media, with assistance, if necessary, from the City's Public Access Officer. Content related to City business shall be maintained in an accessible format and so that it can be produced in response to a request. Wherever possible, such accounts shall clearly indicate that any articles and any other content posted or submitted for posting are subject to public disclosure. Users shall be notified that public disclosure requests must be directed to the relevant Department Head.

6. Maine law and relevant record retention schedules apply to social media formats and social media content. The department maintaining an account shall preserve records required to be maintained pursuant to a relevant records retention schedule for the required retention period on a City server in a format that preserves the integrity of the original record and is easily accessible.

7. Users and visitors to social media accounts shall be notified that the intended purpose of the account is to serve as a mechanism for communication between City employees and members of the public relating to the transaction of City business. City social media account articles and comments containing any of the following forms of content shall not be allowed:

(a) Comments not topically related to the particular social medium article being commented upon;
(b) Profane language or content;
(c) Content that promotes, fosters or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, national origin, physical or mental disability, sexual orientation or any other status protected by law;
(d) Sexual content or links to sexual content;
(e) Solicitations of commerce;
(f) Conduct or encouragement of illegal activity;
(g) Information that may tend to compromise the safety or security of the public or public systems; or
(h) Content that violates a legal ownership interest of any other party.

These guidelines must be displayed to users or made available by hyperlink. Any content removed based on these guidelines must be retained, including the time, date and identity of the poster when available.

8. Administration of City social media accounts.

(a) IT Department staff will maintain a list of social media tools that are approved for use by City departments and staff.
(b) IT Department staff will maintain a list of all City social media accounts. Department Heads must submit to the IT Director a list of all social media accounts maintained by the department, including the following information: (1) the name, hosting site and Internet address and date of inception for the account, and a statement of the purpose and scope of the department's use of the account; (2) all user names, passwords, and other log-in credentials for the account; (3) all authorized social media users for the department that have access to and/or responsibility for the account; and (4) the

administrative contacts and contact information for the account. The Department Head must promptly notify the IT Director of any changes in any of the foregoing, and of any new department social media accounts or pages and any termination of accounts or pages.

(c) Department Heads shall ensure that all department-approved social media accounts and social media content are periodically reviewed for compliance with this policy. Department Heads are responsible for all social media content created, received, transmitted, stored, deleted, destroyed, and/or printed in the name of or on behalf of the City or the department.

(d) The City must be able to immediately edit or remove content from social media accounts.

(e) The City Manager, IT Director, Human Resources Director and Department Heads may monitor content on each of the social media accounts to ensure adherence to this Social Media Policy for appropriate use, message and branding consistent with the goals of City.

(f) Violation of these standards may result in the removal of pages from social media outlets. The IT Director retains the authority to remove information.

9. The City reserves the right to restrict or remove any content that is deemed in violation of this Social Media Policy or any applicable law.

10. The City will approach the use of social media tools as consistently as possible, enterprise-wide.

11. All new social media tools proposed for City use will be approved by the City Manager, IT Director and the appropriate Department Head.