**EUT POLICY ON EMPLOYEE INTERNET USE**

**Amended Work Rule**

NOTE: State information and technology and related communication equipment and resources may include, but are not limited to computer workstations, laptops, mobile devices, voice mail, computer networks, printers, copiers, telephones, fax machines, modems, fax modems, e-mail, local and wide area networks, Internet, and Intranet.

Purpose

The purpose of this policy is to set out the minimum rules to be followed while using any or all of the State-owned or State-leased information and technology equipment and resources under the control of the State of Maine.

Background

The State provides its employees access to I.T. equipment and resources to accomplish tasks, to process, to communicate and to effectively achieve the State of Maine mission, as directed by law and the administration.

State employees should be aware that cell phone, Blackberry and internet messages are generally not secure and can be intercepted by outside parties.[1] Voice mail and e-mail messages may have backup copies that cannot be deleted by the operator. A history of accessed web sites is recorded by most browser software. All of this information may be subject to release under a "Freedom of Access Act" request. The State of Maine and the Office of Information Technology may monitor voice, e-mail, and Internet traffic to improve service levels, enforce this policy, and prevent unauthorized access to State systems.

Unofficial and/or unauthorized use of State-owned equipment places unanticipated and possibly excessive demands on the State's I.T. resources. Accessing unofficial and/or unauthorized sources unnecessarily exposes the State to security risks such as the spread of computer viruses, adware and malware, which may be costly and disruptive to remove.

Maine Freedom of Access Act

The State of Maine "Freedom of Access Act" (1 M.R.S.A., §401-410) clearly provides that any and all written, printed or graphic matter or any mechanical or electronic data compilation (files, notes, records, copies, etc.), regardless of the media used to store or transmit them (paper, film, microfiche, recordable media, electronic media, etc.) in public offices received or prepared for use in connection with the transaction of public governmental business is public property. As such, the public may have access to those materials for examination. The law places some very narrow restrictions on the public access, such as personnel files, certain investigation files, etc. but most materials are subject to public viewing. Employees are advised that there should be no expectation of privacy when using any State-owned I.T. or related communications equipment or resources.

---

1

Work Rules

State-owned I.T. equipment and resources are made available to employees to conduct official State of Maine business. Use of I.T. resources, such as e-mail, Internet, social networking media interfaces such as YouTube, Facebook, and blogs, etc., are intended to be used for State business purposes. The Department's employees are provided with a maine.gov email account through which to conduct state business. All State employees using state-owned I.T. equipment and resources are expected to comply with the following work rules:

1. Unless required to do so in the performance of official duties (e.g., law enforcement), State employees shall not use State-owned, State-leased, or State-controlled I.T. equipment or other resources to create, record, store, copy, transmit, distribute, image, modify, print, download, or display inappropriate or unprofessional materials that demean, denigrate, or harass individuals or groups of individuals, on the basis of race, ethnic heritage, religious beliefs, disability, sexual orientation or gender regardless of whether the material was intended to demean, denigrate or harass any employee or group of employees. This prohibition applies to the use of state-owned equipment regardless of whether the employee is on-duty or off-duty. **Intentional and substantial violations of this work rule are unacceptable and will not be tolerated. As of the effective date of this Work Rule, intentional and substantial violations of this rule shall constitute just cause for termination.**

2. Unless required to do so in the performance of official duties (e.g., law enforcement), State employees shall not use State-owned, State-leased, or State-controlled I.T. equipment or other resources to create, record, store, copy, transmit, distribute, image, modify, print, download, or display materials that are sexually explicit or pornographic in nature. This prohibition applies to the use of State-owned, State-leased, or State-controlled equipment regardless of whether the employee is on-duty or off-duty. **Intentional violations of this work rule – <u>regardless of whether they are of an incidental nature</u> – are unacceptable and will not be tolerated. As of the effective date of this Work Rule, any intentional violation of this rule SHALL constitute just cause for termination.**

3. State employees shall not conduct state business through personal email accounts (e.g., Yahoo, Hotmail, and G-mail)

4. State employees shall not use State's technology resources to forward or otherwise broadcast mass communications that are not work-related, or solicitations for causes unrelated to the State's business, no matter how worthy the cause may be perceived to be. If in doubt as to whether your proposed e-mail meets these guidelines, contact your Human Resources office. Solicitations or mass communications for causes believed to be related to State business should be brief, not endorse any particular product or provider, and should refer readers to a webpage for further information. The Commissioner or his/her designee must approve such solicitations or mass mailings [NOTE: In the Capitol area, Capitol Security must give written permission for solicitations. The Maine State Employees Combined Charitable Appeal is the only solicitation with on-going, or "blanket" approval].

5. State employees shall not use State-owned, leased, or controlled I.T. resources to conduct outside business nor shall they use these resources in conjunction with any outside employment activity.

6. State law makes it a crime to use a computer system operated by a state department or agency to advocate for or against a candidate for federal office, a constitutional office, an elective municipal, county or state office, including leadership positions in the Senate and House of Representatives, as well as to solicit contributions required by law to be reported to the Commission on Governmental Ethics and Election Practice.

7. With the specific exception of accessing pornography as described in Paragraph 2 above, any personal use of State-owned I.T. equipment and resources must be incidental in nature. Examples of incidental use may include but are not limited to , brief e-mails, accessing an appropriate subject on the Internet, phone calls of an urgent nature, using computer capabilities for incidental correspondence, etc.[2] The use of State-owned resources represents a cost to the State and, as such, printing and copying for personal use is restricted to incidental use only. Any personal, incidental use of State-owned I.T. equipment and resources shall not interfere with the Department's business activities, 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 State of Maine, its residents, its taxpayers, or its employees.[3]

8. In the event that an employee inadvertently accesses inappropriate material (to include material deemed as a security risk[4]) the employee is required to immediately secure the material from view. If an employee inadvertently accesses inappropriate or prohibited materials, his or her supervisor or management **must** be advised of the circumstances surrounding the inadvertent access. A failure to notify his or her supervisor or manager will be a factor considered in determining whether the access was intentional or substantial. Employees who advise their supervisors and/or managers of inadvertent access may be held harmless for inadvertently accessing the inappropriate or prohibited materials.

If supervisory or management staff become aware that inappropriate or prohibited materials are being accessed, downloaded, or otherwise transmitted to or by an employee in his or her organization, s/he must act immediately to stop such activity. Supervisors and managers who fail to act immediately to stop such activity will be held accountable for their failure which will include the imposition of disciplinary action up to and including dismissal. Supervisors and managers with questions about how to stop prohibited activity should contact their Director of Human Resources for guidance and consultation.

These rules may be amended as necessary by State policies and procedures.

For further information concerning this policy, contact your Director of Human Resources. For further information technology policies, visit the Office of Information Technology website at http://www.maine.gov/oit/policies.

---

2

3

4

Care should be exercised to avoid inadvertent disclosure of confidential information over these media.
[2] Certain telephone calls and expenses are allowable under the bargaining agreement.
[3] As is the case in other situations, the time associated with any incidental personal use of State-owned I.T. resources must not intrude into an employee's work responsibilities.
[4] http://www.maine.gov/oit/policies/VulnerabilityAssessmentFinal.htm: All State employees who suspect a breach of security has occurred will contact OIT Customer Solutions Center at 624-7700, who will inform the Enterprise Information Security Officer. The Officer will promptly work collaboratively with appropriate AITDs and technical experts to determine the appropriate course of action."

BUREAU OF HUMAN RESOURCES HUMAN RESOURCES POLICY AND PRACTICES MANUAL

## 6.7 PERSONAL USE OF SOCIAL MEDIA

State of Maine agencies (the "State") may use social media[1] technologies to enhance communication, collaboration, and information exchange with citizens in accordance with guidelines and procedures issued by the Office of Information Technology.

The State recognizes that state employees may use social media technology off the job and that such use is subject to certain constitutional and statutory protections. Personal use of social media technologies by state employees that undermines or interferes with the ability of State agencies and state employees to carry out their responsibilities may be the proper subject of State review and corrective action.

The purpose of this policy is to educate state employees that their personal off-duty use of social media technologies may be the proper subject of State review and corrective action where there is a nexus between the personal use and the workplace.

Employees have no expectation of privacy in their use of social media while using any system or device provided by the State or any system or device the cost of which is reimbursed by the State. The State retains the right to monitor, search, access, inspect and read all information contained on any system or device provided or reimbursed by the State. It is the policy of the State of Maine that:

1. Personal use at work: This includes personal use of social media while at work by an employee (e.g. logging onto Facebook and providing personal updates to a Facebook page or Twitter account during work hours using their own or their agency's information technology resources, when such activity is outside of the employee's official job function).

    A. Any such use shall be incidental, shall not interfere with work responsibilities and shall be consistent with the Policy Concerning the Use of State-Owned Information and Technology (I.T.) and Related Communications Equipment and Resources and any additional use policies adopted by the agency.

    B. Excessive personal use of social media during work hours is prohibited.

2. Personal use outside of work: This includes use of social media by an employee in his or her personal capacity outside of work using non-state resources (computers, internet access, e-mail etc.). Any personal use of Social Media ***outside of work*** is subject to First Amendment protections. However, where such personal use is related to subject matter pertinent to State employment, it must be

conducted in such a manner that no impression is created that the employee is speaking on behalf of the Agency.

A. The personal usage identity *must* be distinct from the Agency usage identity, for instance, established under a personal email account, and *not* the State email account.

B. Employees are prohibited from posting information on behalf of a State Agency on the employee's personal *Social Media* page.

C. If an employee identifies himself or herself as a state employee or the employee's personal expression suggests that the employee is an employee of the State, the employee should include a clear disclaimer indicating that the employee is *not* communicating on behalf of the State. The disclaimer should state: "The information on this site is not posted on behalf of the State of Maine," or words to that effect.

D. Employees must refrain from disclosing State confidential information.

E. Employees are prohibited from using their state-issued e-mail address(es) for any personal social media "account," whether based in the World Wide Web or elsewhere.

F. This policy does not extend to, and is not intended to, impair or diminish employees' rights as provided by the State Employees Labor Relations Act or similar laws relating to collective bargaining.

3. State harassment and discrimination policies, confidentiality policies, ethics rules, code of conduct, and workplace violence policies are applicable to all *Social Media* usage.

[1] Social Media is defined as a set of technologies for enabling a community of participants to productively collaborate. It includes blogs; wikis; microblogs such as Twitter™; networking sites/tools such as Facebook™ and LinkedIn™; video sharing sites/tools such as YouTube™; and bookmarking sites/tools such as Del.icio.us™.

~~*040115 JTC*~~
*051915 JTC*