PAUL R. LEPAGE

GOVERNOR

STATE OF MAINE
POLICY AND WORK RULES CONCERNING
THE USE OF STATE INFORMATION AND TECHNOLOGY (I.T.)
EQUIPMENT AND RESOURCES

Amended Work Rule **EFFECTIVE DATE: March 2, 2015**

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.

[1] Care should be exercised to avoid inadvertent disclosure of confidential information over these media.

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.

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 – regardless of whether they are of an incidental nature – 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 Police 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

[2] Certain telephone calls and expenses are allowable under the bargaining agreement.

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]

GUIDELINES AND PROCEDURES

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.

---

[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."