ELECTRONIC COMMUNICATIONS AND INTERNET USE

Number 11.7

Effective Date: March 20, 2015

Supersedes: Policy 11.7, dated August 14, 2009
Policy 11.7, dated September 18, 2007
Policy 11.7, dated July 1, 1999

Subject: ELECTRONIC COMMUNICATIONS AND INTERNET USE

Applicable to: All classified, temporary and exempt employees of the State of Vermont, including all members of the executive branch and members of the boards and commissions who are authorized to use the State Internet service or electronic/wireless communication devices/systems.

Issued By: Department of Human Resources

Approved by: Justin Johnson, Secretary of Administration

PURPOSE AND POLICY STATEMENT

To prescribe rules of conduct and procedure for State employees when using or accessing state government of Vermont (State) owned or provided computers, electronic communication devices/systems. These rules also apply to electronic communications or transactions in which a state employee represents him/herself as a State employee, regardless of whether he or she is using or accessing State equipment.

DEFINITIONS

Access - the ability to enter a system or application or the act of doing so, depending on context.

Agency - a state board, commission, department, agency, or other entity or officer of state government, other than the legislature and the courts.

Agency systems or systems - all agency software, electronic information devices, interconnections, intranet and technical information related to them. Systems include other systems accessed by or through those devices, such as the Internet, email, or telephone services. Systems include designs, specifications, passwords, access codes and encryption codes.

Control - the power held by the Agencies to grant or deny access to all agency systems and the agency's power to trace, review, audit, access, intercept, block, restrict, screen, delete, recover, restore, publish or disclose any information at any time without notice.
Electronic/wireless communication devices or electronic/wireless devices - includes but is not limited to: cellular phones, Blackberries, personal digital assistants (PDAs), and other such mobile devices used to access electronic mail, telephone, and Internet service.

Information - information of any kind, used in any way, in agency systems. Examples include messages, communications, emails, files, records, recordings, transmissions, signals, programs, macros, and data.

POLICY

The State purchases computers, electronic/wireless devices, and Internet services for use by Agencies to meet the operational and programmatic needs of their units. This policy provides guidelines for acceptable access and use, and prohibits any use of systems, the Internet, or electronic or wireless device, by State employees that violates Federal or State laws or regulations.
As defined by this policy, systems and information are State property. Each agency has full control and access as defined above. All systems and information therein are, and shall remain, the property of each agency, subject to its sole control. Each agency owns all legal rights to control, transfer, or use all or any part or product of its systems. All uses must comply with this policy. Nothing in this policy shall be construed to abridge any rights of an agency to control its systems, their uses or information. ***This policy does not impair the right and obligation of Agencies to limit access to systems and records that contain information that is subject to any statutory, regulatory, or common law privilege or obligation to limit access, nor does it alter any agency's rights or obligations under the Vermont public records law (1 V.S.A. § 315, et seq.).***

Authorized Limited Personal Use

Internet, electronic and wireless communication devices and services, and email capabilities are resources to facilitate the work of State government. This policy provides for use by authorized State employees that is consistent with **Personnel Policies and Procedures**, Number 5.6, entitled "Employee Conduct," which states that employees shall not use or attempt to use State personnel, property, or equipment for their private use or for any use not required for the proper discharge of their official duties. That policy has been interpreted to allow a limited degree of personal use of State telephones for private calls when such use meets certain guidelines. Similar allowances will be applied to Internet, electronic and wireless communication devices and services, and email capabilities where personal use meets all of the following tests. No such use will be allowed where any of the following is not met:

- The user must be authorized to use the equipment by management. Managers will exercise reasonable discretion in determining which employees will be denied personal use of Internet or electronic and wireless communication devices and services, including when such use is denied because of abuse or violation of this policy.
- The use must not interfere with an employee's performance of job duties.
- The use must not impose a burden on State resources as a result of frequency or volume of use.
- The use must not otherwise violate this policy, including the prohibition on visiting sites that include potentially offensive or disruptive material. The fact that the use occurs in a private setting or outside of scheduled work hours does not affect this prohibition.

RULES FOR USE OF SYSTEMS OR INTERNET SERVICES

1. Employees with access to systems or the Internet have the responsibility not to disclose their access codes or passwords.
2. Employees are expected to use state-provided systems for state business. Employees with access to a state email account must use their state email account for state business. Employees with state email accounts shall not routinely use personal email accounts to conduct state business unless such use of the employee's personal account is reviewed by the Department of Information and Innovation and approved by the Secretary of Administration. Any use of a non-state-provided system for state business must comply with the State of Vermont's Information Security Policy.
3. Passwords, scramblers or various encryption methods may not be used without agency approval, access and control. No user may attempt to access, copy, forward, delete, or alter the messages of any other user without agency authorization. No agency system may be used to attempt unauthorized access to any information system. No user may use any type of file removal/deletion program on any State computer system without assistance and approval of authorized agency representatives.
4. No employee shall send email that is, or appears to be, sent from another employee's email or that attempts to mask identity. This prohibition does not include email sent with the user's permission that clearly presents the sender's identity.
5. State employees must conform to reasonable professional standards for use of Internet services as detailed in this guideline. This includes a prohibition against any activity that impairs operation of any state computer resource. Such activities include, but are not limited to, sending junk mail such as chain letters, unsolicited commercial email, and/or pyramid schemes, injecting computer viruses or unofficial mass mailings via email. This also includes hacking, which means gaining or attempting to gain unauthorized access to any computers, computer networks, databases, data, or electronically stored information, unless acting within the proper scope of official duties.
6. Employees must be mindful that email messages and other electronic data may be considered public records subject to disclosure under the Vermont Public Records Act (1 V.S.A. § 315, et seq.). In addition, a "public record" is any record produced or acquired in the course of agency business, regardless of whether the record resides in a state-provided system or personal account. 1 V.S.A. § 317(b). Any public record

contained in a non-state-provided system (email or otherwise) is subject to Vermont's Access to Public Records Act.

7. Employees must respect intellectual property rights at all times when obtaining information over the Internet. Copyrighted or licensed information shall be used only with full legal right to do so.

8. Use of the Internet including email is for State business. The only exception is for personal use that fully complies with the limited personal use described by this policy. The use of peer-to-peer (referred to as P2P) networks such as Napster, Kazaa, Gnutella, Grokster, Limewire, and similar services is prohibited. Any use that is not for State business or authorized limited personal use consistent with this policy may result in revocation of Internet access, other appropriate administrative action, or disciplinary or corrective action.

9. Use of agency systems or printers for offensive or disruptive purposes is prohibited. This prohibition includes profanity, vulgarity, sexual content or character slurs. Any inappropriate reference, regardless of whether presented as a statement, language, image, email signature block, audio file, or in any other way that is reasonably likely to be perceived as offensive or disparaging of others on the basis of race, color, age, gender, sexual orientation, gender identity, religions, national origin or disability is also prohibited.

10. An appointing authority of an agency reserves and may exercise all rights relating to information used in its systems. An agency may trace, review, audit, access, intercept, block, restrict, screen, delete, recover, restore, publish or disclose any information used in its systems subject to relevant policies, laws, and regulations.

11. Agencies have the right to monitor their systems and Internet activities of employees. Monitoring may occur in, but is not limited to, circumstances when there is a reason to suspect that an employee is involved in activities that are prohibited by law, violate State policy or regulations, or jeopardize the integrity and/or performance of the computer systems of State government. Monitoring may also occur in the normal course of network administration and trouble-shooting, or on a random basis using electronic tools designed to monitor Internet usage. Agencies must limit access to reports that may be generated by such programs and ensure that records of Internet usage are disclosed to only their appropriate human resources, management, and investigatory staff unless and until it becomes evidence of employee misconduct in which case it is may be used in the same manner and is subject to the same rules of evidence as any other information that is part of a formal investigation into employee conduct. **Agencies must ensure that systems administrators and technicians involved in monitoring, or who otherwise have access to systems and records that contain information that is subject to any statutory, regulatory, or common law privilege or obligation to limit access, are appropriately trained on any requirements to respect such privilege or confidentiality, and directed to comply with such requirements.**

12. Use of fee-for-service providers is not allowed unless the necessary approvals and funding have been obtained in advance. An employee who obligates an agency to pay for services without prior approval may be held personally liable for those costs and may be subject to disciplinary action up to and including dismissal.

13. Prohibited activities also include, but are not limited to the following: lobbying public officials or asking others to lobby in their behalf, printing and/or distributing information from the Internet that is obscene, potentially offensive, harassing, or disruptive.

14. Using or allowing others to use State Internet services or email accounts to conduct transactions or advertising for a personal profit-making business is strictly forbidden. Use of State Internet services for purposes of accessing sites that provide streaming audio or video material for non-work related purposes is prohibited.
15. Use of State computer systems for solicitation for charitable or other causes is prohibited, except for officially-sanctioned activities.

Approved:

Justin Johnson
Secretary of Administration

3/20/2015
Date